ZARZĄDZENIE NR 37/2023

Wójta Gminy Santok

z dnia 15 wrzesnia 2023

w sprawie zatwierdzenia dokumentacji ochrony informacji niejawnych w Urzędzie Gminy Santok".

Na podstawie art. 33 ust. 3 ustawy z dnia 8 marca 1990 r. o samorządzie gminnym (t. j. Dz.U. z 2023 r. poz. 40 ze zm.), w związku z art. 14, art. 15 oraz art. 43 ustawy z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych (t. j. Dz. U. z 2023 r. poz. 756 ze zm.), zarządza się, co następuje:

§ 1. Zatwierdza się „Plan ochrony informacji niejawnych, w tym w razie wprowadzenia stanu nadzwyczajnego w Urzędzie Gminy w Santoku", stanowiący załącznik nr 1 do zarządzenia.

§ 2. Zatwierdza się „Instrukcję dotyczącą sposobu i trybu przetwarzania informacji niejawnych o klauzuli „zastrzeżone" oraz zakres i warunki stosowania środków bezpieczeństwa fizycznego w celu ich ochrony w Urzędzie Gminy w Santoku", stanowiącą załącznik nr 2 do zarządzenia.

§ 3. Zatwierdza się „Dokumentację określającą poziom zagrożeń związanych z nieuprawnionym dostępem do informacji niejawnych lub ich utratą Urzędzie Gminy w Santoku", stanowiącą załącznik nr 3 do zarządzenia.

§ 4. Zatwierdza się „Szacowanie ryzyka dla bezpieczeństwa informacji niejawnych, przetwarzanych w Urzędzie Gminy w Santoku", stanowiącą załącznik nr 4 do zarządzenia.

§ 5. Wykonanie zarządzenia powierza się Pełnomocnikowi ds. Ochrony Informacji Niejawnych.

§ 6. Zarządzenie wchodzi w życie z dniem podpisania.

WÓJT GMINY SANTOK
Paweł Risarek

Uzasadnienie

Zgodnie z ustawą z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych art. 14 Kierownik jednostki organizacyjnej, w której są przetwarzane informacje niejawne, odpowiada za ich ochronę, w szczególności za zorganizowanie i zapewnienie funkcjonowania tej ochrony. W Urzędzie Gminy w Santoku przetwarzane są informacje niejawne o klauzuli „zastrzeżone", w związku z powyższym organizuje się system ochrony informacji niejawnych o klazuli „zastrzeżone". Na system ochrony składają się min. dokumenty stanowiące załączniki do niniejszego zarządzenia.

Załącznik nr 1 do Zarządzenia nr 37/2023 z dnia 15.09.2023r.

URZĄD GMINY W SANTOKU

PLAN OCHRONY INFORMACJI NIEJAWNYCH

w tym w razie wprowadzenia stanu nadzwyczajnego

W URZĘDZIE GMINY W SANTOKU

OPRACOWAŁ:
Pełnomocnik ds. Ochrony
Informacji Niejawnych
Krzysztof Kinal

SANTOK
Wrzesień 2023

Spis treści

Wstęp

Zgodnie z postanowieniami zawartymi w art. 15 ust. 1 pkt 5 ustawy z dnia 5 sierpnia 2010 roku o ochronie informacji niejawnych (Dz. U. z 2023 r. poz. 756. z późn. zm.) do zadań pełnomocnika ds. ochrony informacji niejawnych należy opracowanie i aktualizowanie, wymagającego akceptacji kierownika jednostki organizacyjnej, **planu ochrony informacji niejawnych w jednostce organizacyjnej** i nadzorowanie jego realizacji.

Osoby odpowiedzialne za ochronę informacji niejawnych.

Zgodnie z art.14 ust.1 ustawy z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych (Dz. U. z 2023 r. poz. 756. z późn. zm.) za ochronę informacji niejawnych w Urzędzie Gminy w Santoku, w którym są przetwarzane informacji niejawne, w szczególności za zorganizowanie i zapewnienie funkcjonowania tej ochrony odpowiada wójt gminy. Wójtowi gminy podlega bezpośrednio pełnomocnik do spraw ochrony informacji niejawnych, zwany dalej „Pełnomocnikiem Ochrony", który odpowiada za zapewnienie przestrzegania przepisów o ochronie informacji niejawnych. Pełnomocnik ochrony kieruje grupą pracowników odpowiadających bezpośrednio za bezpieczeństwo informacji niejawnych. W skład tej grupy wchodzą:

- Pełnomocnik ds. Ochrony Informacji Niejawnych,
- Kancelaria Materiałów Niejawnych.

1. Charakterystyka zagrożeń

Biorąc pod uwagę usytuowanie budynku jego konstrukcję oraz funkcję publiczną należy przyjąć możliwość wystąpienia zagrożeń w postaci:

- pożaru,
- powodzi, ulewy lub zalania z innych przyczyn (awaria instalacji),
- wichury,
- katastrofy budowlanej, awarii technicznej,
- demonstracji lub rozruchów ulicznych,
- kradzieży lub aktu wandalizmu,
- ataku terrorystycznego.

W przypadku zaistnienia któregokolwiek z wymienionych powyżej zdarzeń w Urzędzie podjęte zostaną działania zmierzające do zapobieżenia negatywnym ich skutkom określone w osobnych planach zabezpieczających prawidłowe funkcjonowanie obiektu.

W przypadku wprowadzenia przez uprawniony organ wyższych stanów gotowości obronnej państwa uruchomione zostaną procedury przewidziane do realizacji w tych stanach zgodnie z obowiązującymi unormowaniami prawnymi.

2. Opis stref ochronnych i wprowadzonego systemu kontroli dostępu.

Wydzielenie stref ochronnych

W urzędzie Gminy w Santoku wydzielono **strefę ochronną III** – obejmującą pomieszczenie Kancelarii Materiałów Niejawnych (pok. nr 24), w którym przetwarza się, w tym przechowuje, informacje niejawne o klauzuli tajności „zastrzeżone".

Pomieszczenie to spełnia następujące wymagania:

- wyraźnie wskazana w planie ochrony najwyższa klauzula tajności („zastrzeżone") przetwarzanych informacji niejawnych,
- wyraźnie określone i zabezpieczone granice,
- wprowadzony system kontroli dostępu zezwalający na wstęp osób posiadających odpowiednie uprawnienie do dostępu do informacji niejawnych w zakresie niezbędnym do wykonywania pracy,
- w przypadku konieczności wstępu innych osób nieuprawnionych, przetwarzane informacje niejawne zabezpiecza się przed możliwością dostępu

do nich tych osób oraz zapewnia nadzór osoby uprawnionej (pełnomocnik ochrony lub pracownik prowadzący Kancelarię Materiałów Niejawnych).

Opis wprowadzonego systemu kontroli dostępu

System kontroli dostępu obejmuje rozwiązania organizacyjne. Jest oparty na zamkniętych drzwiach pomieszczenia, do którego można uzyskać dostęp za pomocą kluczy wydawanych uprawnionym osobom.

Uprawnienia do wejścia do strefy ochronnej III mają tylko Pełnomocnik Ochrony oraz pracownik prowadzący Kancelarię Materiałów Niejawnych. Osoby nie posiadające uprawnień do wejścia do pomieszczenia Kancelarii Materiałów Niejawnych mogą być wpuszczone do tego pomieszczenia tylko przez Pełnomocnika Ochrony lub pracownika prowadzącego Kancelarię Materiałów Niejawnych.

Prowadzi się rejestr wejścia/wyjścia do/z III strefy bezpieczeństwa. Wzór rejestru stanowi załącznik nr 4.

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

Uprawnienia dostępu do strefy ochronnej III można otrzymać tylko w przypadku stałego zatrudnienia w strefie ochronnej III.

Pełnomocnik Ochrony oraz pracownik prowadzący Kancelarię Materiałów Niejawnych są na stałe zatrudnieni w strefie III. Pozostali pracownicy Urzędu mogą przebywać w strefie ochronnej III pod nadzorem osób zatrudnionych w strefie.

Pozbawienie uprawnień dostępu do strefy ochronnej III nastąpi obligatoryjne w związku z:

- zwolnieniem się z pracy na własną prośbę,
- zwolnieniem z pracy przez pracodawcę,
- upływem ważności poświadczenia bezpieczeństwa, względnie nie uzyskaniem ponownego poświadczenia bezpieczeństwa,
- przeniesieniem na inne stanowisko, na którym nie ma potrzeby dostępu do stref ochronnych,
- przebywaniem (ponad 6 miesięcy) na bezpłatnym urlopie, zwolnieniu lekarskim czy urlopie macierzyńskim itp.

W wyżej wymienionych przypadkach Pełnomocnik Ochrony odbiera uprawnienia dostępu do strefy ochronnej III.

Pracownik ma obowiązek niezwłocznego poinformowania Pełnomocnika Ochrony o zagubieniu klucza do pomieszczenia strefy ochronnej III. Obowiązek aktualizowania listy uprawnionych spoczywa na Pełnomocniku Ochrony.

- **Procedura przyjmowania interesantów**

Obsługa interesantów może odbywać się w strefie ochronnej III gdy osoby zatrudnione w tej strefie nie przetwarzają informacji niejawnych. Interesanci mogą przebywać w strefie za zgodą Pełnomocnika Ochrony lub pracownika prowadzącego Kancelarię Materiałów Niejawnych pod warunkiem zabezpieczenia informacji niejawnych w sposób uniemożliwiający ich przypadkowe ujawnienie.

- **Ochrona fizyczna budynku**

W budynku Urzędu nie ma ochrony fizycznej. Na parterze przy wejściu znajduje się punk obsługi interesanta. W Urzędzie zamontowany jest system alarmowy. System jest uzbrajany po godzinach pracy. System monitoruje licencjonowania agencja ochrony.

Wstęp do pomieszczeń lub przebywania na terenie Urzędu jest możliwy po godzinach pracy Urzędy tylko w przypadku zgody bezpośredniego przełożonego. Praca może odbywać się do godz. 20, do czasu skończenia pracy przez osoby sprzątające.

- **Przebywanie osób nieuprawnionych w strefie ochronnej**

Sprzątanie, serwisowanie systemu alarmowego, prace remontowe i konserwacyjne w Kancelarii Materiałów Niejawnych mogą się odbywać tylko w obecności osób zatrudnionych w strefie ochronnej III.

Na czas wykonywania prac pracownicy zabezpieczają dokumenty niejawne w szafie zamykając je na klucz lub zabezpieczają dokumenty niejawne w sposób uniemożliwiający przypadkowe ujawnienie ich treści osobom nieuprawnionym. Prace w ww. pomieszczeniu, należy planować w taki sposób, aby były one prowadzone na zasadach „czystego biurka". Wstęp do strefy ochronnej III innych osób nieuprawnionych możliwy jest za zgodą Pełnomocnika Ochrony lub pracownika prowadzącego Kancelarię Materiałów Niejawnych.

Wstęp do pomieszczenia zlokalizowanego w strefie ochronnej III podczas nieobecności etatowych pracowników jest możliwy wyłącznie komisyjnie, przez osoby posiadające stosowne poświadczenie bezpieczeństwa lub upoważnienie. Z faktu komisyjnego otwarcia pomieszczeń w strefie ochronnej III, należy sporządzić „Protokół z przeprowadzenia czynności związanych z dostępem do pomieszczeń (urządzeń) będących w III strefie ochronnej" – stanowiący załącznik nr 3 do niniejszego planu.

4. Zastosowane środki bezpieczeństwa fizycznego

Zabezpieczenia mechaniczne.

Do zabezpieczeń mechanicznych zastosowanych do zabezpieczenia ochrony informacji niejawnych w strefie ochronnej III należy zaliczyć:

- **Drzwi wejściowe:**
  - **Strefa Ochronna III – Kancelaria materiałów niejawnych (pok. nr 24)** - drzwi do pomieszczenia przeciwpożarowe (drzwi o zwiększonej odporności na włamanie)
  - Wejście poprzez pomieszczenie Pełnomocnika Ochrony.
- **Ściany i stropy**

  Wykonane z materiałów niepalnych, spełniających wymagania w zakresie klasy odporności pożarowej oraz nośności granicznej odpowiadającej wymaganiom określonym w rozporządzeniu Rady Ministrów w sprawie środków bezpieczeństwa fizycznego stosowanych do zabezpieczenia informacji niejawnych.
- **Okna**

  Pomieszczenia zlokalizowane w strefie III posiadają okna tradycyjne. Od wewnątrz zastosowano żaluzje zabezpieczające przed podglądem. Wysokość nad powierzchnią gruntu wynosi 3,9 m.
- **Szafy stalowe**

  Szafa stalowa na dokumenty spełnia co najmniej wymagania klasy A. Wyrób spełnia wymagania stawiane szafom do przechowywania dokumentów niejawnych zgodnie z Kryteriami Technicznymi KT/101/IMP/2004(5) oraz zgodnie z Rozporządzeniem Rady Ministrów z dnia 18.10.2005 r. w sprawie organizacji i funkcjonowania kancelarii tajnych. Na szafę producent wydał Certyfikat Zgodności Nr P41/012/2006 (1983). Zgodnie z § 10 ust 2 Rozporządzenia Rady Ministrów z dnia 29 maja 2012 r. w sprawie środków bezpieczeństwa fizycznego stosowanych do zabezpieczania informacji niejawnych, certyfikaty i tabliczki znamionowe przyznane wyposażeniu i urządzeniom służącym ochronie informacji niejawnych, wydane przed dniem wejścia w życie rozporządzenia, zachowują ważność.
- **Instalacje elektryczne**

  Instalacje odbiorcze gniazdowe i oświetleniowe

W strefie ochronnej III zainstalowano obwód gniazdowy 230V zasilany przewodem z izolacją na napięcie robocze 750 V. Jako ochronę podstawową od porażeń zastosowano izolowanie części będących pod napięciem.

Punkty odbiorcze

W strefie ochronnej III zainstalowano gniazda wtyczkowe 230V oraz sufitowe wypusty oświetleniowe sterowane przez dwubiegunowy łącznik oświetlenia.

Urząd wyposażony jest centralny UPS APC o mocy 15kVA oraz agregat prądotwórczy Pramac GSW45Y, moc maksymalna: 46,4kVA / 37,12kW, moc nominalna 41,97kVA / 33,58kW

- **System kontroli dostępu**

System kontroli dostępu obejmuje rozwiązania organizacyjne. Jest oparty na zamkniętych drzwiach pomieszczenia, do którego można uzyskać dostęp za pomocą kluczy wydawanych uprawnionym osobom.

- **System wykrywania pożaru**

Urząd nie posiada systemu wykrywania pożaru.

- **System monitoringu**

Zastosowany system monitoringu obejmuje: 5 kamer wokół budynku oraz 1 w środku skierowaną na wejście. Zapis jest przechowywany do 14 dni. (zalecany okres przechowywania 30)

5. Procedury bezpieczeństwa dla strefy ochronnej III

- **Klauzule tajności informacji niejawnych przetwarzanych w strefie ochronnej III**

  W Urzędzie Gminy w Santoku przetwarza się informacje o klauzuli tajności „zastrzeżone". Informacje niejawne o klauzuli „zastrzeżone" można przetwarzać wyłącznie w pomieszczeniu zlokalizowanym w strefie ochronnej III - pomieszczenie Kancelarii Materiałów Niejawnych (pok. nr 24).

- **Osoby upoważnione do wejścia do strefy ochronnej III**

  Do przebywania w pomieszczeniu zlokalizowanym w strefie ochronnej III upoważnieni są dysponenci tego pomieszczenia – pracownik prowadzący Kancelarię Materiałów Niejawnych i Pełnomocnik Ochrony. W strefie mogą przebywać osoby posiadające stosowne poświadczenie bezpieczeństwa lub upoważnienie pod nadzorem pełnomocnika ochrony lub pracownika prowadzącego Kancelarię Materiałów Niejawnych.

- **Procedury dotyczące nadzoru osoby uprawnionej lub ochrony informacji niejawnych w przypadku wejścia do strefy ochronnej III osób innych niż wskazane wyżej**

  Wstęp uprawnionych osób do pomieszczeń zlokalizowanych w strefie ochronnej III może nastąpić po uzyskaniu zgody pracownika prowadzącego Kancelarię Materiałów Niejawnych lub Pełnomocnika Ochrony. Każdorazowe wejście do strefy ochronnej III uprawnionego wykonawcy dokumentów, dokumentowane jest w „Rejestrze wejścia/wyjścia do/z III strefy bezpieczeństwa." Upoważnieniem do wejścia do pomieszczenia Kancelarii Materiałów Niejawnych jest aktualny „Wykaz osób upoważnionych do dostępu do informacji niejawnych w Urzędzie Gminy w Santoku", prowadzony przez Pełnomocnika Ochrony.

  Ponadto w strefie ochronnej III mogą przebywać osoby posiadające stosowne poświadczenie bezpieczeństwa lub upoważnienie wydane przez Wójta Gminy Santok uprawniające do dostępu do informacji niejawnych o klauzuli „zastrzeżone". Osoby nie będące pracownikami Urzędu mogą przebywać w tej strefie za zgodą Wójta Gminy Santok lub upoważnionej przez niego osoby lub Pełnomocnika Ochrony lub pracownika prowadzącego Kancelarię Materiałów Niejawnych pod nadzorem upoważnionego pracownika pod warunkiem

zabezpieczenia informacji niejawnych w sposób uniemożliwiający ich przypadkowe ujawnienie.

Wstęp do pomieszczeń zlokalizowanych w strefie ochronnej III podczas nieobecności etatowych pracowników jest możliwy wyłącznie komisyjnie, przez osoby posiadające stosowne poświadczenie bezpieczeństwa lub upoważnienie.

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

- **Klucze do Kancelarii Materiałów Niejawnych**

  Wyodrębniono trzy komplety kluczy do Kancelarii Materiałów Niejawnych:

  – Pierwszy komplet użytku bieżącego jest zawsze w posiadaniu pracownika prowadzącego Kancelarię Materiałów Niejawnych, który używa go do zamykania i otwierania Kancelarii Materiałów Niejawnych.

  – Drugi komplet kluczy do Kancelarii Materiałów Niejawnych jest w posiadaniu Pełnomocnika Ochrony.

  – Trzeci komplet kluczy „zapasowych" zdeponowany jest w „bezpiecznej kopercie" w sejfie u Wójta Gminy Santok.

  W razie zagubienia (utraty) kluczy do Kancelarii Materiałów Niejawnych, należy bezzwłocznie dokonać wymiany zamków.

- **Klucze do szafy stalowej w Kancelarii Materiałów Niejawnych**

  Wyodrębniono dwa komplety kluczy do szafy stalowej, w której przechowuje się materiały niejawne o klauzuli „zastrzeżone":

  – Pierwszy komplet kluczy użytku bieżącego jest zawsze w posiadaniu osoby prowadzącej Kancelarię Materiałów Niejawnych, która używa go do zamykania i otwierania szafy. Po zakończeniu pracy klucze zamykane są w Kancelarii Materiałów Niejawnych.

  – Drugi komplet kluczy „zapasowych" jest zdeponowany w „bezpiecznej kopercie" w sejfie u Wójta Gminy Santok.

- **Dodatkowy sejf w szafie stalowej w Kancelarii Materiałów Niejawnych**

  – Pierwszy komplet kluczy użytku bieżącego jest zawsze w posiadaniu Pełnomocnika Ochrony.

  – Drugi komplet kluczy „zapasowych" zdeponowany jest w „bezpiecznej kopercie" w sejfie u Wójta Gminy Santok.

- **Klucze do pomieszczenia nr 23 stanowiącego przedpokój do Kancelarii Materiałów Niejawnych**

  Wyodrębniono trzy komplety kluczy do pomieszczenia 23:

  – dwa komplety użytku bieżącego (po jednym) jest zawsze w posiadaniu Pełnomocnika Ochrony i osoby prowadzącej Kancelarię Materiałów Niejawnych, którzy używają go do zamykania i otwierania pomieszczenia,

- trzeci komplet kluczy „zapasowych" zdeponowany jest w „bezpiecznej kopercie" w sejfie u Wójta Gminy Santok. Można go wydać tylko Pełnomocnikowi Ochrony i osobie prowadzącej Kancelarię Materiałów Niejawnych za pokwitowaniem oraz uprawnionemu członkowi komisji, na polecenie Wójta Gminy Santok. W razie zagubienia (utraty) kluczy należy bezzwłocznie dokonać wymiany zamków.

- **Zasady komisyjnego otwierania pomieszczenia Kancelarii Materiałów Niejawnych zlokalizowanej w strefie ochronnej III**

  Komisyjne otwarcie Kancelarii Materiałów Niejawnych może mieć miejsce wyłącznie za zgodą Wójta Gminy Santok według następujących zasad:

  - każdy członek komisji musi posiadać ważne poświadczenie bezpieczeństwa lub upoważnienie upoważniające do dostępu do informacji niejawnych o klauzuli „zastrzeżone",
  - skład osobowy komisji winien wynosić co najmniej dwie osoby,
  - otwarcie pomieszczeń odbywa się z wykorzystaniem kluczy zapasowych zdeponowanych u Wójta Gminy Santok,
  - z faktu pobrania kluczy zapasowych oraz z przeprowadzanych czynności sporządzany jest niezwłocznie protokół zawierający przyczynę pobrania kluczy zapasowych, przyczynę otwarcia pomieszczeń strefy ochronnej III, podjęte czynności, członków komisji i ich podpisy.

  Protokół sporządza się w 3 egzemplarzach po jednym dla Wójta Gminy Santok, Pełnomocnika Ochrony i osoby prowadzącej Kancelarię Materiałów Niejawnych – wzór stanowi załącznik nr 3.

7. Procedury reagowania na zagrożenia

Całodobową ochronę obiektu zapewnia firma ochroniarska. Po godzinach pracy Urzędu monitorowane są sygnały z systemu alarmowego. W razie potrzeby wysyłany jest patrol interwencyjny. Informowany jest Pełnomocnik Ochrony oraz inne odpowiedzialne osoby funkcyjne Urzędu.

W przypadku wystąpienia zagrożeń o większej skali powiadamiane są stosowne służby (Policja, Straż Pożarna, Agencja Bezpieczeństwa Wewnętrznego).

W przypadku otrzymania informacji o podłożeniu ładunku wybuchowego lub wprowadzenia na terenie kraju lub województwa stopni alarmowych, decyzje co do dalszego funkcjonowania Urzędu zgodnie z procedurami podejmuje Wójt Gminy Santok.

W przypadku podnoszenia stanów gotowości obronnej państwa na polecenie Wójta Gminy Santok następuje przemieszczenie Urzędu, w tym pomieszczenia, w którym są przetwarzane informacje niejawne, zgodnie z planem przemieszczenia Urzędu do Zapasowego Miejsca Pracy.

W przypadku stwierdzenia naruszenia w urzędzie przepisów o ochronie informacji niejawnych o klauzuli „zastrzeżone" Pełnomocnik Ochrony zawiadamia o tym Wójta Gminy Santok i podejmuje niezwłocznie działania zmierzające do wyjaśnienia okoliczności tego naruszenia oraz ograniczenia jego negatywnych skutków.

8. Instrukcja postepowania w przypadku uzyskania informacji o ujawnieniu lub bezprawnym wykorzystaniu informacji niejawnych

Ustawa o ochronie informacji niejawnych nakłada na każdego obowiązek ochrony informacji niejawnych przed nieuprawnionym ujawnieniem, niezależnie od formy i sposobu ich wyrażania, także w trakcie ich opracowania. Bezpośrednią odpowiedzialność za ochronę informacji niejawnych w jednostce ponoszą kierownik jednostki oraz Pełnomocnik Ochrony. Osoby te nie ponoszą jednak bezpośredniej odpowiedzialności za świadome lub nieświadome naruszenie przepisów przez poszczególnych pracowników. Zatem obowiązek ochrony informacji niejawnych spoczywa na każdym, kto w posiadanie takich informacji wszedł, niezależnie czy nastąpiło to w sposób uprawniony czy też przypadkowy.

Z treści artykułu art. 266 Kodeksu Karnego wynika że:

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

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

§ 3. Ściganie przestępstwa określonego w § 1 następuje na wniosek pokrzywdzonego.

Zgodnie z treścią art. 17 ust. 1 ustawy o ochronie informacji niejawnych w przypadku stwierdzenia naruszenia w jednostce organizacyjnej przepisów o ochronie informacji niejawnych Pełnomocnik Ochrony zawiadamia o tym kierownika jednostki organizacyjnej, podejmuje niezwłocznie działania zmierzające do wyjaśnienia okoliczności tego naruszenia oraz ograniczenia jego negatywne skutki. Działania te mają charakter postępowania wyjaśniającego.

Naruszenie przepisów o ochronie informacji niejawnych w Urzędzie Gminy w Santoku może wystąpić w formie:

- próby zabrania dokumentów przez pracownika Urzędu,

- próby powielania dokumentów, kserowania lub kopiowania dokumentów w inny sposób,
- zagubienia posiadanego dokumentu,
- rozpoznawania organizacji pracy Kancelarii Materiałów Niejawnych,
- próby wglądu do dokumentów przez osoby nieuprawnione,
- przekazywania informacji osobom postronnym przez pracownika mającego prawo wglądu do dokumentów niejawnych i zapoznawania się z ich treścią,
- włamania lub wyłudzenie dostępu (wejście w posiadanie kluczy od pomieszczeń) przez osobę nieupoważnioną.

Prowadzone postepowanie wyjaśniające powinno mieć na celu wyjaśnienie wszystkich okoliczności zdarzenia i polegać na przeprowadzeniu następujących czynności:

- uzyskanie potwierdzenia informacji o naruszeniu przepisów,
- poinformowanie kierownika jednostki,
- powołaniu komisji do przeprowadzenia postepowania wyjaśniającego,
- przesłuchaniu osób mających wiedzę na temat zaistniałego zdarzenia,
- ustalenie wykazu utraconych dokumentów lub treści przekazanych informacji,
- ustalenie sposobu wejścia osób niepowołanych w posiadanie,
- przeprowadzenie innych czynności w zależności od potrzeb,
- ustalenie ewentualnych winnych naruszenia,
- ustalenia skali szkód wyrządzonych ujawnieniem.

Wymienione powyżej czynności przeprowadza powołana przez kierownika jednostki komisja której przewodzi Pełnomocnik Ochrony. Osoby wchodzące w skład komisji powinny posiadać poświadczenie bezpieczeństwa lub upoważnienie dostępu do dokumentów niejawnych o klauzuli „zastrzeżone".

Jeżeli do ujawnienia doszło wskutek włamania komisja zabezpiecza pomieszczenia uniemożliwiając w ten sposób zacieranie śladów i powiadamia Policję.

W przypadku przejęcia postępowania przez Policję lub Agencję Bezpieczeństwa Wewnętrznego komisja postępuje zgodnie z zaleceniami tych organów, a orzeczenia tych organów stanowią podstawę zakończenia postępowania.

Z przeprowadzenia czynności zabezpieczających lub po zakończeniu własnego postępowania wyjaśniającego komisja sporządza protokół w którym zawarte są wszelkie ustalenia w danej sprawie. Protokół powinien zostać zakończony wnioskami

wskazującymi ewentualnych sprawców naruszenia oraz rozmiar wyrządzonych szkód.

Protokół powinien zawierać również rozwiązania uniemożliwiające powstanie tego typu ujawnień w przyszłości. Stanowi on również podstawę do wyciągnięcia wobec winnych ujawnienia stosownych wniosków dyscyplinarnych.

W przypadku utraty dokumentów o klauzuli „zastrzeżone" kierownik jednostki na podstawie ustaleń komisji określa stopień szkody, jaką ponosi społecznie uzasadniony interes lub stopień niebezpieczeństwa ujawnienia tajemnicy oraz podejmuje decyzję co do dokumentów zagubionych, jeżeli taka utrata miała miejsce.

9. Plany awaryjne uwzględniające potrzebę ochrony informacji niejawnych w razie wprowadzenia stanów nadzwyczajnych, w celu zapobieżenia utraty poufności, integralności lub dostępności informacji niejawnych

a) Za stan nadzwyczajny w rozumieniu niniejszego dokumentu uważa się wymienione w art.228 Konstytucji RP sytuacje takie jak:
   - **Stan wojenny:** w rozumieniu przepisów ustawy o stanie wojennym oraz kompetencjach Naczelnego Dowódcy Sił Zbrojnych i zasadach jego podległości konstytucyjnym organom Rzeczypospolitej Polskiej z dnia 29 sierpnia 2002r. (Dz.U. z 2022 poz. 2091 t.j. ze zm.),
   - **Stan wyjątkowy:** w rozumieniu przepisów ustawy o stanie wyjątkowym z dnia 21 czerwca 2002 r. (Dz.U. z 2017 r. poz. 1928 t.j. ze zm.),
   - **Stan klęski żywiołowej:** w rozumieniu przepisów ustawy o stanie klęski żywiołowej z dnia 18 kwietnia 2002 r. (Dz.U. z 2017 r. poz. 1897 t.j. ze zm.).

b) Plan określa zasady postępowania w sytuacji konieczności zabezpieczenia materiałów niejawnych będących w posiadaniu urzędu, w czasie wprowadzenia na terenie jej działania stanu nadzwyczajnego.

c) Szczególnej ochronie w związku z podjętymi działaniami podlegają materiały:
   - mające bezpośredni związek z funkcjonowaniem jednostki organizacyjnej w warunkach zagrożenia,
   - mające związek z realizacją zadań obronnych i Siłami Zbrojnymi.

d) Zabezpieczenie dokumentów, o których mowa w planie, dokonuje się poprzez ich ewakuowanie z pomieszczenia Kancelarii Materiałów Niejawnych. Ewakuacja tych dokumentów następuje w warunkach pozwalających doprowadzić je do ulokowania w miejscu zapewniającym im odpowiednie bezpieczeństwo w zaistniałej sytuacji zagrożenia, możliwie spełniające wymogi ustawy o ochronie informacji niejawnych i stosownie do występującego ryzyka.

e) Ewakuacja dokumentów następuje na podstawie pisemnego polecenia Wójta Gminy Santok lub upoważnionej osoby. Koordynatorem ewakuacji jest Pełnomocnik Ochrony.

f) Miejsce zabezpieczenia materiałów niejawnych podlegających ewakuacji określony jest w planie przemieszczenia Urzędu do ZMP. Dokumentacja ta stanowi informację niejawną.
g) Nadzór i ochronę transportu do nowego miejsca przechowywania sprawują Pełnomocnik Ochrony wraz z pracownikiem Kancelarii Materiałów Niejawnych.
h) Zabezpieczeniu poprzez ewakuację podlegają wszystkie materiały niejawne, jeżeli ich ilość jest niewielka.
i) W przypadku większej ilości dokumentów należy brać pod uwagę zapisy pkt. c.
j) Pozostałe dokumenty należy ewakuować, o ile czas i warunki na to pozwalają lub w uzgodnieniu z właściwym Archiwum na pisemne polecenie Wójta Gminy Santok zniszczyć lub przekazać do właściwego Archiwum.
k) W stanie nadzwyczajnym sporządza się dwa egzemplarze spisu materiałów przeznaczonych do ewakuacji oraz niepodlegających ewakuacji, z których w razie ewakuacji jeden egzemplarz pozostawia się na stanowisku pracy, natomiast drugi egzemplarz jest zabierany wraz z ewakuowanymi materiałami do miejsca ewakuacji i nowego miejsca pracy.
l) Zabezpieczenie ewakuowanych dokumentów odbywa się poprzez dokonanie następujących czynności:
   - wydanie przez Wójta Gminy Santok lub innej osoby upoważnionej stosownych poleceń Pełnomocnikowi Ochrony,
   - jeżeli ewakuacja zarządzona jest w godzinach pozasłużbowych osoba podejmująca decyzję o ewakuacji zarządza wezwanie osób odpowiedzialnych przy pomocy wszelkich dostępnych środków,
   - zapewnienie niezbędnego środka transportu oraz pracowników w ilości niezbędnej do zapakowania i przemieszczenia materiałów wymagających ewakuacji,
m) W przypadku nieobecności osoby prowadzącej Kancelarię Materiałów Niejawnych, Pełnomocnik Ochrony w porozumieniu z kierownikiem jednostki, wyznacza dwuosobową komisję spośród pracowników Urzędu posiadających uprawnienia dostępu do informacji niejawnych, która dokona komisyjnego otwarcia pomieszczenia oraz szafy.
n) Komisja realizująca powyższe zadania sporządza protokół z dokonanych czynności, który będzie opisywał:

- zasadność otwarcia pomieszczenia i szafy pod nieobecność osoby prowadzącej Kancelarię Materiałów Niejawnych,
- określenie rodzaju i ilości materiałów podlegających zabezpieczeniu i ewakuacji,
- określenie rodzajów materiałów, które nie będą brane pod uwagę w trakcie ewakuacji,
- określenie sposobu zabezpieczenia ewakuowanych materiałów w nowym miejscu przechowywania,
- wskazanie sposobu zabezpieczenia materiałów, które nie podlegają ewakuacji.

o) W celu skutecznego i sprawnego działania dla realizacji Planu w Urzędzie materiały niejawne:
- przechowywane są tylko w strefie ochronnej III,
- szafa, w której są przechowywane informacje niejawne jest trwale oznakowana,
- worki ewakuacyjne są przechowywane w miejscu widocznym, dostępnym i nie wymagającym kluczy.

p) Realizację postanowień zawartych w planie powierza się pracownikowi prowadzącemu Kancelarię Materiałów Niejawnych w zakresie:
- przygotowania materiałów będących w zasobach Urzędu, do ewentualnego zabezpieczenia,
- bieżącego gromadzenia materiałów, z uwzględnieniem ewentualnej ewakuacji i ich zabezpieczenia.

Załączniki

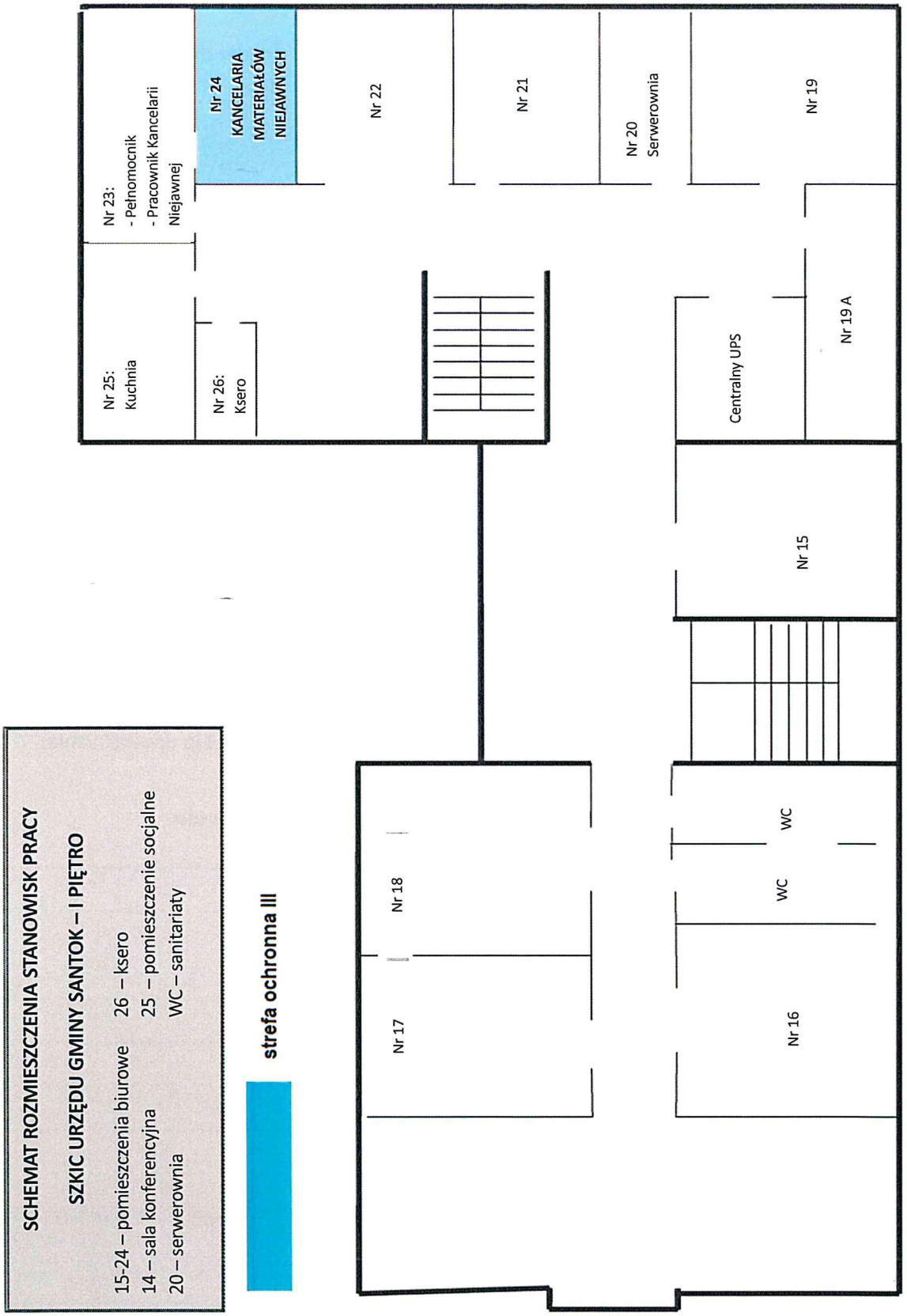
Załącznik nr 1 – Schemat lokalizacji Urzędu Gminy;

Załącznik nr 2 – Podział na strefy ochronne;

Załącznik nr 3 – Wzór „Protokołu z przeprowadzenia czynności związanych z dostępem do pomieszczeń będących w strefie ochronnej;

Załącznik nr 4 – wzór rejestru wejść/wyjść do strefy bezpieczeństwa.

Załącznik nr 1


SCHEMAT ROZMIESZCZENIA STANOWISK PRACY
SZKIC URZĘDU GMINY SANTOK – I PIĘTRO
15-24 – pomieszczenia biurowe
14 – sala konferencyjna
20 – serwerownia
26 – ksero
25 – pomieszczenie socjalne
WC – sanitariaty
strefa ochronna III
Nr 25: Kuchnia
Nr 23: - Pełnomocnik - Pracownik Kancelarii Niejawnej
Nr 24 KANCELARIA MATERIAŁÓW NIEJAWNYCH
Nr 26: Ksero
Nr 22
Nr 21
Nr 20 Serwerownia
Nr 19
Centralny UPS
Nr 19 A
Nr 15
Nr 17
Nr 18
WC
WC
Nr 16

Załącznik nr 3

Protokół

z przeprowadzenia czynności związanych z dostępem do pomieszczeń będących w III strefie ochronnej.

ZEZWALAM

na komisyjne wejście do strefy ochronnej III – pomieszczenie nr 24

.....

(pieczęć i podpis Wójta Gminy Santok, data)

Zgodnie z decyzją Wójta Gminy Santok komisja w składzie:

- przewodniczący .....
(Imię i nazwisko, nr poświadczenia bezpieczeństwa lub upoważnienia)
- członkowie .....
(Imię i nazwisko, nr poświadczenia bezpieczeństwa lub upoważnienia)

.....
(Imię i nazwisko, nr poświadczenia bezpieczeństwa lub upoważnienia)

.....
(Imię i nazwisko, nr poświadczenia bezpieczeństwa lub upoważnienia)

dokonała wejścia do pomieszczenia wymienionego powyżej w celu:

.....

.....

W pomieszczeniu wykonano następujące czynności:

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

Pobrano następujące dokumenty:

L.p.	Nazwa dokumentu, przedmiotowej teczki i jej numer	Numer ewidencyjny	Ilość egzemplarzy	Nr egzemplarza	Uwagi
1.	2.	3.	4.	5.	7.

Szafę stalową i drzwi wejściowe pomieszczenia oplombowano pieczęcią Przewodniczącego Komisji nr ..... .

Imiona i nazwiska oraz podpisy:

Przewodniczący.....

Członkowie .....

.....

.....

Załącznik nr 4

REJESTR WEJŚĆ/WYJŚĆ DO STREFY BEZPIECZEŃSTWA

lp	*Imię i nazwisko*	*Data*	*Godzina*		*Podpis*	*Uwagi*
			wejście	*wyjście*		
1	*2*	*3*	*4*	*5*	*6*	*7*

Załącznik nr 2 do Zarządzenia nr 37/2023 z dnia 15.09.2023r.

URZĄD GMINY W SANTOKU

INSTRUKCJA

DOTYCZĄCA SPOSOBU I TRYBU PRZETWARZANIA INFORMACJI NIEJAWNYCH O KLAUZULI „ZASTRZEŻONE" ORAZ ZAKRES I WARUNKI STOSOWANIA ŚRODKÓW BEZPIECZEŃSTWA FIZYCZNEGO W CELU ICH OCHRONY W URZĘDZIE GMINY W SANTOKU

OPRACOWAŁ:
Pełnomocnik ds. Ochrony Informacji Niejawnych
Krzysztof Kinal

SANTOK
Wrzesień 2023

Spis treści

I. PRZEDMIOT OCHRONY

- Informacje niejawne oznaczone klauzulą „zastrzeżone",
- pomieszczenia, w których przetwarzane są informacje niejawne o klauzuli „zastrzeżone".

II. SZACOWANIE RYZYKA

1. W ramach systemu bezpieczeństwa fizycznego informacji niejawnych stosuje się środki bezpieczeństwa fizycznego w celu zapewnienia poufności, integralności i dostępności tych informacji.
2. W celu doboru adekwatnych środków bezpieczeństwa fizycznego określa się poziom zagrożeń związanych z utratą poufności, integralności lub dostępności informacji niejawnych, zwany dalej „poziomem zagrożeń".
3. Poziom zagrożeń określono dla obszaru, w którym przetwarzane są informacje niejawne.
4. Poziom zagrożeń określa się jako niski, średni lub wysoki.
5. W celu określenia poziomu zagrożeń przeprowadzono analizę, w której uwzględniono wszystkie istotne czynniki mogące mieć wpływ na bezpieczeństwo informacji niejawnych, w szczególności:
   - klauzule tajności przetwarzanych informacji niejawnych,
   - postać i ilość informacji niejawnych,
   - sposób przechowywania informacji niejawnych,
   - otoczenie i strukturę budynków lub obszarów, w których przetwarzane są informacje niejawne,
   - ilość osób mających lub mogących mieć dostęp do informacji niejawnych, a także posiadane przez nich uprawnienia oraz uzasadnioną potrzebę dostępu do informacji niejawnych,
   - szacowane zagrożenie ze strony obcych służb specjalnych oraz zagrożenie sabotażem, zamachem terrorystycznym, kradzieżą lub inną działalnością przestępczą.
6. Poziom zagrożeń określa się przed rozpoczęciem przetwarzania informacji niejawnych, a także po każdej zmianie czynników, mogącej mieć istotny wpływ na bezpieczeństwo informacji niejawnych.

7. W zależności od poziomu zagrożeń określonego w wyniku przeprowadzenia analizy, stosuje się odpowiednią kombinację następujących środków bezpieczeństwa fizycznego:
   - **bariery fizyczne** – środki chroniące granice miejsca, w którym przetwarzane są informacje niejawne, w szczególności są to ogrodzenia, ściany, bramy, drzwi i okna;
   - **systemy sygnalizacji włamania i napadu** – stosowane w celu podwyższenia poziomu bezpieczeństwa, który dają bariery fizyczne, a w pomieszczeniach i budynkach w celu zastąpienia lub wsparcia pracowników jednostki organizacyjnej lub personelu bezpieczeństwa,
   - **kontrola dostępu** – stosowana w celu zagwarantowania, że dostęp do chronionego obszaru uzyskują wyłącznie osoby posiadające odpowiednie uprawnienia,
   - **personel bezpieczeństwa** – osoby przeszkolone, nadzorowane, a w razie konieczności posiadające odpowiednie uprawnienie dostępu do informacji niejawnych, zatrudnione w celu wykonywania czynności związanych z fizyczną ochroną informacji niejawnych, w tym kontroli dostępu, nadzoru nad systemem monitoringu wizyjnego, a także reagowania na alarmy lub sygnały awaryjne,
   - **system monitoringu wizyjnego** – stosowany przez pracowników jednostki organizacyjnej lub personel bezpieczeństwa w celu bieżącego monitorowania ochronnego lub sprawdzania incydentów bezpieczeństwa i sygnałów alarmowych pochodzących z systemów sygnalizacji włamania i napadu,
   - **szafy i zamki** – stosowane do przechowywania informacji niejawnych lub zabezpieczające te informacje przed nieuprawnionym dostępem,
   - **system kontroli osób i przedmiotów** - polegający na użyciu odpowiednich urządzeń technicznych lub zwracaniu się o dobrowolne poddanie się kontroli lub udostępnienie do kontroli rzeczy osobistych, a także przedmiotów wnoszonych lub wynoszonych – stosowany w celu zapobiegania próbom nieuprawnionego wnoszenia na chroniony obszar rzeczy zagrażających bezpieczeństwu informacji niejawnych lub nieuprawnionego wynoszenia informacji niejawnych z budynków lub obiektów.
8. W celu zapewnienia poufności, integralności i dostępności informacji niejawnych można zastosować również środki bezpieczeństwa fizycznego inne niż wymienione powyżej, jeżeli wynika to z analizy poziomu zagrożeń.

9. Jeżeli istnieje zagrożenie podglądu, także przypadkowego, informacji niejawnych, podejmuje się środki w celu wyeliminowania takiego zagrożenia.
10. Dokumentacja określająca poziom zagrożeń związanych z nieuprawnionym dostępem do informacji niejawnych lub ich utratą została zatwierdzona przez kierownika jednostki.

III. EWIDENCJA MATERIAŁÓW NIEJAWNYCH

1. Informacje niejawne oznaczone klauzulą „zastrzeżone" są ewidencjonowane w Kancelarii Materiałów Niejawnych.
2. Informacje niejawne o klauzuli „zastrzeżone" mogą być ewidencjonowane na zasadach określonych przez kierownika jednostki, opisanych w Instrukcji.
3. Dokumenty niejawne wpływające do Urzędu ewidencjonuje się w dzienniku ewidencyjnym.
4. Dokumenty niejawne wytworzone – wychodzące z Urzędu rejestruje się w dzienniku ewidencyjnym.
5. Każdy dokument niejawny przychodzący lub wychodzący z Urzędu ewidencjonuje się w odrębnej pozycji dziennika ewidencyjnego.
6. Numer ewidencyjny każdego dokumentu niejawnego stanowiącego o klauzuli „zastrzeżone" powinien być poprzedzony skrótem literowym „Z".
7. Ewidencjonowaniu podlegają wszystkie materiały niejawne oznaczone klauzulą „zastrzeżone".
8. Osoba prowadząca Kancelarię Materiałów Niejawnych jest odpowiedzialna za ewidencjonowanie materiałów niejawnych, przyjmuje przesyłki za pokwitowaniem i odciska na nich pieczęć oraz datę wpływu do Urzędu.
9. Osoba prowadząca Kancelarię Materiałów Niejawnych przyjmując przesyłkę, sprawdza:
   - prawidłowość adresu,
   - całość opakowania,
   - zgodność odcisku pieczęci na opakowaniu z nazwą jednostki organizacyjnej nadawcy.
10. W przypadku stwierdzenia uszkodzenia przesyłki lub śladów jej otwierania osoba kwitująca odbiór przesyłki sporządza, wraz z doręczającym, protokół uszkodzenia. Jeden egzemplarz protokołu przekazuje się nadawcy, drugi - pełnomocnikowi ochrony w jednostce organizacyjnej odbiorcy, a w przypadku gdy w obiegu przesyłek pośredniczył przewoźnik - kolejny egzemplarz protokołu przekazuje się także jemu.

11. Osoba prowadząca Kancelarię Materiałów Niejawnych:
    - sprawdza, czy zawartość przesyłki odpowiada wyszczególnionym na niej numerom ewidencyjnym,
    - ustala, czy liczba załączników i stron jest zgodna z liczbą oznaczoną na poszczególnych dokumentach.
12. W przypadku stwierdzenia nieprawidłowości w wyniku czynności, o których mowa w pkt.10, pracownik sporządza w dwóch egzemplarzach protokół z otwarcia przesyłki zawierający opis nieprawidłowości, jeden egzemplarz przekazując do kancelarii nadawcy.
13. Osoba prowadząca Kancelarię Materiałów Niejawnych odnotowuje fakt sporządzenia protokołu, o którym mowa w pkt. 10 i 12, w odpowiednim dzienniku lub rejestrze w rubryce "Informacje uzupełniające/Uwagi".

IV. ZABEZPIECZENIE INFORMACJI NIEJAWNYCH

1. Informacje niejawne oznaczone klauzulą „zastrzeżone" mogą być przetwarzane w strefie ochronnej III, których granice zostały określone w „Planie ochrony informacji niejawnych, w tym w razie wprowadzenia stanu nadzwyczajnego".
2. Szczegółowy wykaz pomieszczeń, w których przetwarza się informacje o klauzuli „zastrzeżone" zawiera załącznik nr 3 do instrukcji.
3. Szczegółowy opis zabezpieczeń zawarty jest w „Planie ochrony informacji niejawnych, w tym w razie wprowadzenia stanu nadzwyczajnego" oraz w „Dokumentacji określającej poziom zagrożeń związanych z nieuprawnionym dostępem do informacji niejawnych lub ich utratą".

V. DOSTĘP DO INFORMACJI NIEJAWNYCH

1. Informacje niejawne oznaczone klauzulą „zastrzeżone" mogą być udostępniane wyłącznie osobie uprawnionej do dostępu do informacji niejawnych o określonej klauzuli niejawności.
2. Uzyskanie uprawnień dostępu do informacji niejawnych o klauzuli „zastrzeżone" może nastąpić:
    - po uzyskaniu przez pracownika upoważnienia do dostępu do informacji niejawnych oznaczonych klauzulą „zastrzeżone" wydanego przez kierownika jednostki lub posiadaniu poświadczenia bezpieczeństwa,

- po przeszkoleniu danej osoby w zakresie ochrony informacji niejawnych i uzyskaniu odpowiedniego zaświadczenia.

3. Osoba przeszkolona, o którym mowa w pkt. 1 i 2, zgodnie z art.20 ust.1 ustawy o ochronie informacji niejawnych składa pisemne oświadczenie o zapoznaniu się z przepisami o ochronie informacji niejawnych.

VI. KANCELARIA MATERIAŁÓW NIEJAWNYCH

1. W urzędzie funkcjonuje Kancelaria Materiałów Niejawnych, która została utworzona dla potrzeb jednostki, dla właściwego przechowywania, ewidencjonowania oraz obiegu materiałów niejawnych oznaczonych klauzulą „zastrzeżone".
2. Organizacja pracy Kancelarii Materiałów Niejawnych zapewnia możliwość ustalenia w każdych okolicznościach, gdzie znajduje się materiał o klauzuli „zastrzeżone" pozostający w dyspozycji urzędu oraz kto z tym materiałem się zapoznał.
3. Osoba prowadząca Kancelarię Materiałów Niejawnych odmawia udostępnienia lub wydania materiału osobie nieuprawnionej.
4. W celu uniemożliwienia osobom nieuprawnionym dostępu do informacji niejawnych o klauzuli „zastrzeżone":
   - zorganizowano strefy ochronne,
   - wprowadzono system kontroli wejść i wyjść ze stref ochronnych,
   - określono uprawnienia do przebywania w strefach ochronnych,
   - zastosowano wyposażenie i urządzenia służące ochronie informacji niejawnych, którym przyznano certyfikaty.
5. Pracą i obsługą Kancelarii Materiałów Niejawnych zajmuje się pracownik zatrudniony na stanowisku ds. zarządzania kryzysowego.
6. Do podstawowych zadań osoby prowadzącej Kancelarię Materiałów Niejawnych należy:
   - bezpośredni nadzór nad obiegiem dokumentów,
   - udostępnianie lub wydawanie dokumentów osobom do tego uprawnionym,
   - egzekwowanie zwrotu dokumentów,
   - prowadzenie bieżącej kontroli postępowania z dokumentami,
   - wykonywanie poleceń Pełnomocnika Ochrony.
7. W przypadku zmiany na stanowisku osoby prowadzącej Kancelarię Materiałów Niejawnych sporządza się protokół zdawczo-odbiorczy.
8. Protokół, o którym mowa w pkt. 7, sporządza się w obecności pracownika zdającego obowiązki, osoby przejmującej obowiązki oraz Pełnomocnika Ochrony. Protokół

sporządza się w dwóch egzemplarzach; pierwszy egzemplarz przechowywany jest w Kancelarii Materiałów Niejawnych, drugi – u Pełnomocnika Ochrony.

9. W przypadku czasowej nieobecności osoby prowadzącej Kancelarię Materiałów Niejawnych jej obowiązki przejmuje Pełnomocnik Ochrony. W razie jego braku kancelarię przejmuje inny pracownik wyznaczony pisemnie przez kierownika jednostki.
10. W pomieszczeniu Kancelarii Materiałów Niejawnych jest wydzielone miejsce, w którym osoby upoważnione mogą zapoznawać się z dokumentami i materiałami.
11. Dokumenty i materiały oznaczone klauzulą "zastrzeżone" oraz bez klauzuli tajności są przechowywane w oddzielnych teczkach, chyba że wchodzą one w skład zbioru dokumentów.
12. Po zakończeniu pracy osoba prowadząca Kancelarię Materiałów Niejawnych jest obowiązana sprawdzić prawidłowość zamknięcia szaf i pomieszczenia Kancelarii Materiałów Niejawnych.
13. Wszelkie nieprawidłowości związane z naruszeniem zasad, określonych powyżej należy niezwłocznie zgłaszać Pełnomocnikowi Ochrony.
14. W Kancelarii Materiałów Niejawnych przyjmuje się, rejestruje, przechowuje, przekazuje i wysyła dokumenty oraz prowadzi:
    - rejestr dzienników ewidencji i teczek,
    - dziennik ewidencyjny,
    - książkę doręczeń przesyłek miejscowych.
15. W przypadkach uzasadnionych organizacją ochrony informacji niejawnych Kancelaria Materiałów Niejawnych może prowadzić także inne rejestry niż wyżej wymienione.

VII. POSTĘPOWANIE Z PRZESYŁKAMI

1. Stanowisko ds. sekretariatu w Referacie Organizacyjno-Administracyjnego zajmuje się przyjmowaniem, rozdziałem i wysyłką korespondencji w Urzędzie.
2. Stanowisko ds. sekretariatu nie otwiera przesyłek zawierających informacje niejawne.
3. Stanowisko ds. sekretariatu odbiera przesyłkę i odciska na niej pieczęć oraz datę wpływu do jednostki organizacyjnej.
4. Przyjmując przesyłkę, sprawdza się:
    - prawidłowość adresu,
    - całość pieczęci i opakowania,

- zgodność odcisku pieczęci na opakowaniu z nazwą jednostki nadawcy,
- zgodność numeru na przesyłce z numerem tej przesyłki w wykazie, książce doręczeń a także na zwrotnym potwierdzeniu odbioru.

5. W przypadku stwierdzenia przesyłki zawierającej informacje niejawne informowany jest pracownik prowadzący Kancelarię Materiałów Niejawnych lub Pełnomocnik Ochrony.
6. W przypadku stwierdzenia uszkodzenia przesyłki lub śladów jej otwierania pracownik prowadzący Kancelarię Materiałów Niejawnych sporządza, wraz z doręczającym, protokół uszkodzenia. Jeden egzemplarz protokołu przekazuje się nadawcy, drugi pełnomocnikowi ochrony w jednostce organizacyjnej odbiorcy, a w przypadku gdy w obiegu przesyłek pośredniczył przewoźnik – kolejny egzemplarz protokołu przekazuje się także jemu.
7. Po otwarciu przesyłki pracownik prowadzący Kancelarię Materiałów Niejawnych:
   - sprawdza, czy zawartość przesyłki odpowiada wyszczególnionym na niej numerom ewidencyjnym,
   - ustala, czy liczba załączników i stron jest zgodna z liczbą oznaczoną na poszczególnych dokumentach.
8. W przypadku stwierdzenia nieprawidłowości pracownik prowadzący Kancelarię Materiałów Niejawnych sporządza w dwóch egzemplarzach protokół z otwarcia przesyłki zawierający opis nieprawidłowości, jeden egzemplarz przekazując do kancelarii nadawcy.
9. Pracownik prowadzący Kancelarię Materiałów Niejawnych odnotowuje fakt sporządzenia protokołu, w odpowiednim dzienniku lub rejestrze w rubryce „Informacje uzupełniające/Uwagi".
10. Pracownik prowadzący Kancelarię Materiałów Niejawnych nie otwiera przesyłek oznaczonych „do rąk własnych". W odpowiednim dzienniku lub rejestrze wpisuje nadawcę, numer i datę wpływu dokumentu w rubryce „Informacje uzupełniające/Uwagi" odnotowuje się, że przesyłka była oznaczona „do rąk własnych".
11. Na opakowaniu przesyłek „do rąk własnych", wpisuje się datę wpływu, pozycję i numer, pod którym zarejestrowano przesyłkę. Przesyłkę przekazuje się – za pokwitowaniem – bezpośrednio adresatowi, a w razie jego nieobecności – osobie przez niego upoważnionej do odbioru.
12. Zatrzymanie przez adresata dokumentu, adresowanego „do rąk własnych", odnotowuje się w rubryce „Informacje uzupełniające/Uwagi".

13. W przypadku zwrotu do Kancelarii Materiałów Niejawnych przesyłki adresowanej „do rąk własnych", pracownik prowadzący Kancelarię Materiałów Niejawnych uzupełnia dane dotyczące przesyłki w odpowiednim dzienniku lub rejestrze.
14. Jeżeli adresat podjął decyzję o przechowywaniu przesyłki „do rąk własnych" w stanie zamkniętym, pracownik prowadzący Kancelarię Materiałów Niejawnych dokonuje czynności, o których mowa w pkt. 12, przy udziale adresata. Przesyłka jest w takim przypadku przechowywana w formie zapieczętowanego pakietu, a fakt ten odnotowuje się w rubryce „Informacje uzupełniające/Uwagi".
15. Przesyłki pilne, telegramy i szyfrogramy doręcza się adresatom bezzwłocznie. Przy kwitowaniu odbioru tych przesyłek odnotowuje się godzinę doręczenia.
16. Otrzymaną i wysłaną przesyłkę bądź wytworzony dokument rejestruje się odpowiednio w kolejności wytworzenia lub otrzymania.
17. Wszelkich adnotacji, w dziennikach ewidencyjnych, dokonuje się tuszem w kolorze niebieskim lub czarnym. Zmian dokonuje się kolorem czerwonym, umieszczając datę, imię i nazwisko oraz podpis dokonującej zmiany.
18. Zabrania się wycierania, zamazywania lub nadpisywania zapisów danych w dziennikach ewidencji.
19. Wysyłka dokumentów niejawnych odbywa się za pośrednictwem Stanowiska ds. sekretariatu.
20. Pracownik prowadzący Kancelarię Materiałów Niejawnych przygotowuje przesyłkę zgodnie z § 8 Rozporządzenia Prezesa Rady Ministrów z dnia 7 grudnia 2011 r. w sprawie nadawania, przyjmowania, przewożenia, wydawania i ochrony materiałów zawierających informacje niejawne.
21. Przygotowana przesyłkę pracownik prowadzący Kancelarię Materiałów Niejawnych przekazuje na Stanowisko ds. sekretariatu.
22. Stanowisko ds. sekretariatu przekazuje przesyłkę przewoźnikowi na podstawie wykazu przesyłek nadanych.
23. Pracownik prowadzący Kancelarię Materiałów Niejawnych odnotowuje w dzienniku ewidencyjnym numer z rejestru przesyłek wychodzących z Urzędu.

VIII. OBOWIĄZKI PRACOWNIKA PROWADZĄCEGO KANCELARIĘ MATERIAŁÓW NIEJAWNYCH

1. Przed otwarciem drzwi sprawdzić stan zamków i zabezpieczenie drzwi pomieszczenia.

2. Sprawdzić stan zabezpieczeń szaf, sprzętu biurowego.
3. Przestrzegać zasad zakazu wstępu w miejsca wydzielone osobom nieuprawnionym.

IX. ZAKRES UDOSTĘPNIANIA INFORMACJI NIEJAWNYCH

Udostępnianie informacji niejawnych oznaczonych klauzulą „zastrzeżone" może nastąpić w oparciu o ważne poświadczenie bezpieczeństwa lub pisemne upoważnienie kierownika jednostki, ważne szkolenie z zakresu ochrony informacji niejawnych oraz w zakresie niezbędnym do wykonywania obowiązków służbowych.

X. ZASADY WYKONYWANIA DOKUMENTÓW NIEJAWNYCH

1. Klauzulę tajności nadaje osoba, która jest uprawniona do oznaczenia dokumentu lub innego niż dokument materiału.
2. Propozycje przyznania klauzuli tajności na wykonywanym dokumencie przedstawia osoba sporządzająca dokument.
3. Dokumenty niejawne powinny być opisane i oznaczone zgodnie z Rozporządzeniem Prezesa Rady Ministrów z dnia 22 grudnia 2011 r., w sprawie sposobu oznaczania materiałów, umieszczania na nich klauzul tajności, (Dz.U.2011 nr 288 z 2011, poz.1692).
4. Dopuszcza się odstępstwa od sposobu oznaczania materiałów niejawnych określonych w Rozporządzeniu wymienionym w pkt 3 jeżeli istnieją inne przepisy szczegółowe regulujące wykonywanie tych dokumentów. Np. dokumentacja obronna tworzona na podstawie podręcznika normalizacji obronnej.
5. Przykładowy sposób oznaczenia dokumentów zawiera załącznik nr 1.

XI. WYKONYWANIE DOKUMENTÓW NIEJAWNYCH W SYSTEMACH TELEINFORMATYCZNYCH

1. Systemy teleinformatyczne, w których mają być przetwarzane informacje niejawne, podlegają akredytacji bezpieczeństwa teleinformatycznego.
2. Bezpieczeństwo teleinformatyczne zapewnia się przed rozpoczęciem oraz w trakcie przetwarzania informacji niejawnych w systemie teleinformatycznym.

XII. NADAWANIE, ZMIANA I ZNOSZENIE KLAUZULI TAJNOŚCI MATERIAŁOM NIEJAWNYM.

1. Klauzulę tajności nadaje osoba, która jest uprawniona do podpisania dokumentu lub oznaczenia innego niż dokument materiału.
2. Informacje niejawne podlegają ochronie w sposób określony w ustawie o ochronie informacji niejawnych do czasu zniesienia lub zmiany klauzuli tajności.
3. Osoba wymieniona w pkt.1 może określić datę lub wydarzenie, po którym nastąpi zniesienie lub zmiana klauzuli tajności.
4. Zniesienie lub zmiana klauzuli tajności jest możliwe wyłącznie po wyrażeniu pisemnej zgody przez osobę, o której mowa w pkt.1, albo jej przełożonego w przypadku ustania lub zmiany ustawowych przesłanek ochrony.
5. Należy nie rzadziej niż raz na 5 lat dokonać przeglądu materiałów celem ustalenia, czy spełniają ustawowe przesłanki ochrony.
6. Po zniesieniu lub zmianie klauzuli tajności podejmuje się czynności polegające na naniesieniu odpowiednich zmian w oznaczeniu materiału i poinformowaniu o nich odbiorców. Odbiorcy materiału, którzy przekazali go kolejnym odbiorcom, są odpowiedzialni za poinformowanie ich o zniesieniu lub zmianie klauzul tajności.
7. Oznaczenie materiału klauzulą tajności polega na umieszczeniu na nim klauzul tajności.
8. Przyznaną klauzulę tajności nanosi się w sposób wyraźny i w pełnym jej brzmieniu.

ZAŁĄCZNIKI DO INSTRUKCJI

Załącznik Nr 1 - Przykład oznaczania dokumentu niejawnego o klauzuli „zastrzeżone".

Załącznik Nr 2 - Wzór upoważnienia uprawniającego do dostępu do informacji niejawnych oznaczonych klauzulą „zastrzeżone".

Załącznik nr 3 – Wykaz pomieszczeń, w których przetwarza się informacje o klauzuli „zastrzeżone".

Kolorem czerwonym zaznaczono możliwość odstąpienia od oznaczeń zgodnie z art. 5 Rozporządzenia

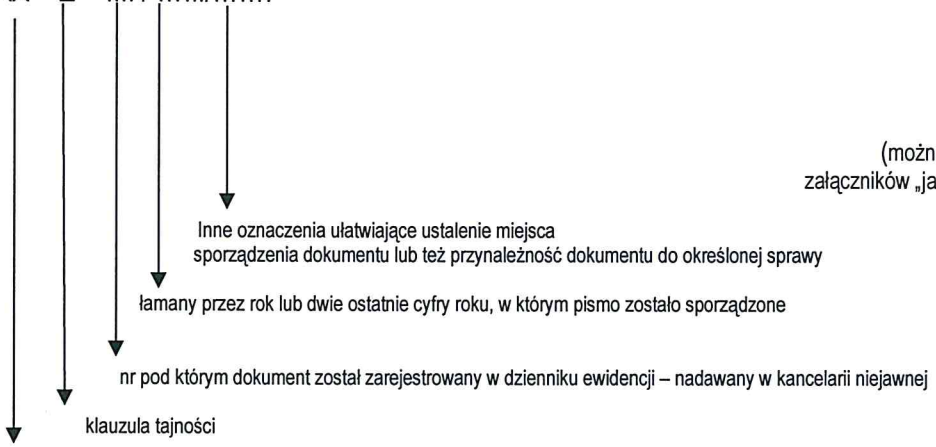
ZASTRZEŻONE

……
nazwa jednostki lub komórki organizacyjnej

XX – Z - …. / ……/…….

Santok,……

Egz. Nr ……
(lub Egz. pojedynczy)
(można wnieść dyspozycję po odłączeniu załączników „jawne po odłączeniu załączników")



(nazwa stanowiska adresata)
…… …….. ……

……
(imię i nazwisko)(lub adresaci wg rozdzielnika)

……
(nazwa miejscowości)

Treść pisma (dokumentu)

……
……
……
……

Bezpośrednio pod treścią pisma:
Załączniki – Ilość załączników: (np. 3 na 13 str.)
Zał. 1 – zastrzeżony XX – Z - …. / ..../……. na 2 str. (Egz. nr……/)
Zał. 2 – zastrzeżony XX – Z - …. / ..../……. na 5 str. (Egz. nr……/)
Zał. 3 – jawny na 6 str. Tylko adresat

……
(stanowisko, imię i nazwisko podpis osoby upoważnionej)

Wykonano w 2 egz.

Egz. Nr 1 – adresat
Egz. Nr 2 – a/a
(lub adresaci wg rozdzielnika)
Wykonał:……

Strona nr 1 z 1

ZASTRZEŻONE
(klauzula tajności, numer strony
oraz liczba stron całego dokumentu)

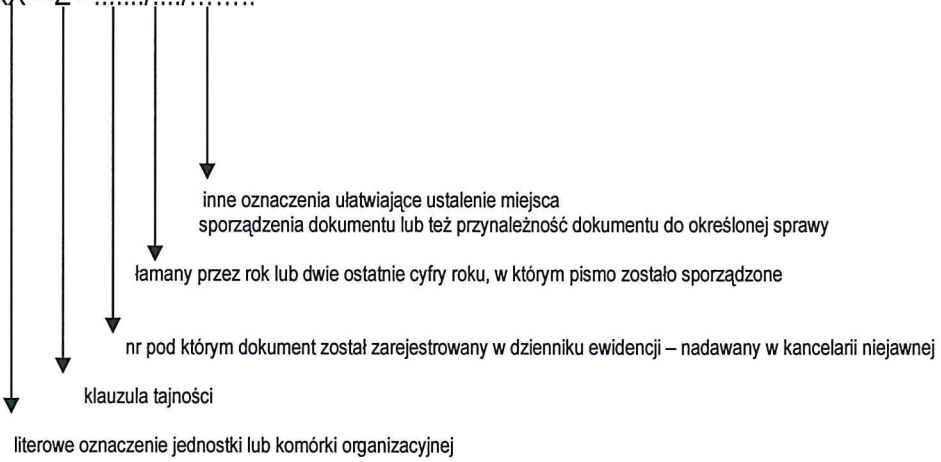
PRZYKŁAD OZNACZANIA ZAŁĄCZNIKA DO PISMA O KLAUZULI ZASTRZEŻONE

Załącznik Nr……do dokumentu……. z dnia ……

ZASTRZEŻONE

……
nazwa jednostki lub komórki organizacyjnej

XX – Z - ……./…./……..



Santok, dnia……
Egz. Nr ……
(lub Egz. pojedynczy)

Nazwa Załącznika

Treść Dokumentu

……
……
……
……

Strona nr 1 z 2

ZASTRZEŻONE

WZÓR ZAŁĄCZNIKA DO PISMA O KLAUZULI ZASTRZEŻONE Str. 2

ZASTRZEŻONE

Egz. Nr……

XX - Z - ..../..../……

Treść Dokumentu Ciąg Dalszy

……
……
……

Bezpośrednio pod treścią.

……
(stanowisko, imię i nazwisko podpis osoby upoważnionej)

Wykonano w 2 Egz.

Egz. Nr 1 – adresat
Egz. Nr 2 – a/a
(lub adresaci wg rozdzielnika)
Wykonał:……

Załącznik Nr 2 - Wzór upoważnienia uprawniającego do dostępu do informacji niejawnych oznaczonych klauzulą „zastrzeżone”

Santok, dnia …….

……

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

UPOWAŻNIENIE NR POI-……/Z/20…….

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 2023 r., poz. 756 t. j. ze zm.) upoważniam do dostępu do informacji niejawnych oznaczonych klauzulą tajności „zastrzeżone” następującą osobę:

1. Imię

   .....

2. Nazwisko (w tym przybrane)

   .....

3. Nr PESEL

   .....

4. Imię ojca

   .....

5. Uwagi:

   .....

Niniejsze upoważnienie wydane jest w celu wykonywania obowiązków służbowych na stanowisku związanym z dostępem do informacji niejawnych o klauzuli „zastrzeżone”.

Upoważnienie wygasa z chwilą zakończenia stosunku pracy, o ile nie zostanie odwołane wcześniej.

……..……..
Pieczątka i podpis kierownika jednostki organizacyjnej

Załącznik nr 3 – Wykaz pomieszczeń, w których przetwarza się informacje o klauzuli „zastrzeżone".

l.p.	Nr. Pokoju
1	24 Kancelaria Materiałów Niejawnych

Załącznik nr 3 do Zarządzenia nr 37/2023 z dnia 15.09.2023r.

URZĄD GMINY W SANTOKU

DOKUMENTACJA
OKREŚLAJĄCA POZIOM ZAGROŻEŃ ZWIĄZANYCH Z NIEUPRAWNIONYM DOSTĘPEM DO INFORMACJI NIEJAWNYCH LUB ICH UTRATĄ W URZĘDZIE GMINY W SANTOKU

OPRACOWAŁ:
Pełnomocnik ds. Ochrony Informacji Niejawnych
Krzysztof Kinal

SANTOK
Wrzesień 2023

1. Wstęp

Podstawą opracowania przedmiotowej dokumentacji są zapisy zawarte w artykule 45 ustawy z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych (Dz.U. z 2023r. poz. 756 t. j.) oraz w rozporządzeniu Rady Ministrów z dnia 29 maja 2012 r. (Dz.U.2012, poz. 683 z dnia 19 czerwca 2012 r.) w sprawie środków bezpieczeństwa fizycznego stosowanych do zabezpieczenia informacji niejawnych.

2. Podstawowe zasady bezpieczeństwa

W celu prawidłowego zabezpieczenia informacji niejawnych, w tym doboru odpowiednich środków bezpieczeństwa fizycznego należy określić poziom zagrożeń nieuprawnionego ujawnienia lub utraty informacji niejawnych. Określenie poziomu zagrożeń jest indywidualną oceną znaczenia następujących rodzajów zagrożeń:

a) zagrożenia naturalne, których źródła nie leżą w zachowaniu człowieka, wynikające z działania sił przyrody lub awarii urządzeń,
b) zagrożenia związane z umyślnym i nieumyślnym zachowaniem człowieka.

Czynniki te mają lub mogą mieć wpływ na bezpieczeństwo informacji niejawnych w Urzędzie. Generalną zasadą bezpieczeństwa materiałów niejawnych jest ochrona informacji przed nieuprawnionym dostępem, zniszczeniem lub ujawnieniem. Bezpieczeństwo materiałów niejawnych osiąga się poprzez zastosowanie odpowiednich przedsięwzięć obejmujących środki fizyczne, organizacyjne, osobowe i techniczne w celu zapewnienia ochrony fizycznej oraz kontroli dostępu do określonych stref ochronnych. Przedsięwzięcia te mają na celu zmniejszenie ryzyka do poziomu akceptowalnego, a tym samym zapewnienie odpowiedniego stanu bezpieczeństwa materiałów niejawnych.

Przy podejmowaniu przedsięwzięć związanych z bezpieczeństwem materiałów niejawnych należy wziąć pod uwagę czynniki, których zakres może się różnić w zależności od:

a) lokalizacji jednostki organizacyjnej i dyslokowanych w niej poszczególnych stref ochronnych,
b) zastosowanych środków ochrony fizycznej, ochrony osobowej i wykorzystanych systemów elektronicznych,
c) liczby osób mających dostęp do informacji niejawnych,
d) ilości dokumentów przetwarzanych w Urzędzie,
e) zastosowanego zabezpieczenia przed zagrożeniem pożarem,

f) konstrukcji budynków i pomieszczeń, w których są przechowywane i udostępniane materiały niejawne,

g) innych czynników wynikających ze specyfiki Urzędu.

Przedsięwzięcia te dla zapewnienia bezpieczeństwa materiałów powinny zawierać:

a) organizację i zarządzanie bezpieczeństwem,

b) bezpieczeństwo fizyczne,

c) bezpieczeństwo osobowe,

d) bezpieczeństwo materiałów niejawnych,

e) wyposażenie i urządzenia służące ochronie informacji niejawnych, którym przyznano certyfikaty,

f) uprawnienia do przebywania w strefach ochronnych,

g) kontrolę wejść i wyjść ze stref ochronnych.

Zarządzanie ryzykiem jest procesem ciągłym, wprowadzonym na etapie projektowania i organizacji systemu ochrony informacji niejawnych. Jego celem jest utrzymanie ryzyk na poziomie akceptowalnym.

Analiza ryzyka jest procesem okresowym i może być zainicjowana w dowolnym okresie, pozwalając na zweryfikowanie istniejących zagrożeń i obszarów wymagających zabezpieczeń. Proces analizy ryzyka polega na identyfikacji ryzyk tzn. prawdopodobieństwa wystąpienia określonych zagrożeń, określeniu ich wielkości i wpływu na bezpieczeństwo, a także opisaniu obszarów wymagających zabezpieczenia i zastosowania odpowiednich środków ochrony.

3. Zasady określania poziomu zagrożeń

W celu doboru właściwych środków bezpieczeństwa fizycznego określa się poziom zagrożeń związanych z utratą poufności, dostępności lub integralności informacji niejawnych.

Poziom zagrożeń ocenia się jako wysoki, średni lub niski oraz określa się dla pomieszczenia lub obszaru, w którym przetwarzane są informacje niejawne.

W celu określenia poziomu zagrożeń przeprowadzono analizę, w której uwzględniono istotne czynniki mogące mieć wpływ na bezpieczeństwo informacji niejawnych, a w szczególności:

a) klauzule tajności przetwarzanych informacji niejawnych,

b) postać i ilość informacji niejawnych,

c) sposób przechowywania informacji niejawnych,

d) otoczenie i strukturę budynków lub obszarów, w których przetwarzane są informacje niejawne,
e) ilość osób mających lub mogących mieć dostęp do informacji niejawnych, a także posiadane uprawnienia oraz uzasadnioną potrzebę dostępu do informacji niejawnych,
f) inne czynniki wynikające ze specyfiki Urzędu.

Określając poziom zagrożenia ustalono realne zagrożenia mogące mieć wpływ na bezpieczeństwo informacji niejawnych, a także przyjęto następujące założenia:

a) W celu prawidłowego zabezpieczenia informacji niejawnych, w tym doboru odpowiednich środków bezpieczeństwa fizycznego określono poziom zagrożeń nieuprawnionym ujawnieniem lub utratą informacji niejawnych. Określenie poziomu zagrożeń jest indywidualną oceną znaczenia czynników mogących mieć wpływ na bezpieczeństwo informacji niejawnych w Urzędzie. Ocena przedstawionych czynników leży w sferze odpowiedzialności Wójta Santoka.
b) Każdy z wymienionych czynników był poddany wnikliwej analizie pod kątem jego znaczenia dla zagrożenia ujawnieniem lub utrata informacji niejawnych. Ocena poziomu zagrożeń uwzględniająca klauzule tajności przetwarzanych informacji niejawnych determinuje stosowanie odpowiednich środków bezpieczeństwa fizycznego.
c) Przy określaniu poziomu zagrożeń oceniono znaczenie danego czynnika dla bezpieczeństwa informacji niejawnych w Urzędzie, a nie sam czynnik jako taki.
d) Poziom zagrożeń ustalono na podstawie wyboru „Oceny istotności czynnika" mającego wpływ na ujawnienie lub utratę informacji niejawnych w Urzędzie. Z uzasadnienia oceny (sporządzonej według wskazań przedstawionych w tabelach oceny istotności czynników zagrożeń) wynika, jakie znaczenie dla Urzędu ma konkretny czynnik (istotny lub mało istotny), a nie w jaki sposób czy jakimi środkami bezpieczeństwa fizycznego zabezpieczono informacje niejawne. Wynik dokonanej analizy miał zasadnicze znaczenie dla określenia poziomu zagrożeń w zależności od tego czy wskazane w „Tabelach oceny istotności czynników zagrożeń" czynniki bierze się pod uwagę jako: „bardzo istotne, istotne albo mało istotne" dla zagrożenia ujawnieniem lub utrata informacji niejawnych.

e) W tabelach oceny istotności czynników zagrożeń wskazano czynniki mające lub mogące mieć wpływ na bezpieczeństwo informacji niejawnych.

f) Każdy z czynników podlegał indywidualnej ocenie pod kątem znaczenia dla zagrożenia ujawnieniem lub utratą informacji niejawnych w Urzędzie. Wybór uzasadniono.

g) Wartości punktowe przypisano odpowiednio „ocenie istotności" tj. czynnik oceniony jako „bardzo istotny" 8 pkt, „istotny" – 4 pkt, „mało istotny" – 1 pkt. Liczba punktów nie podlega modyfikacji.

h) Liczbę punktów podsumowano w „Tabeli określającej poziom zagrożenia". Uzyskany wynik wskazał poziom zagrożenia, zgodnie ze skalą określoną w „Tabeli do określania poziomów zagrożeń":

Poziom zagrożeń		
NISKI	ŚREDNI	WYSOKI
7 pkt – 16 pkt	17 pkt – 32 pkt	powyżej 32 pkt

OCENA ISTOTNOŚCI

CZYNNIKÓW ZAGROŻEŃ

MAJĄCYCH LUB MOGĄCYCH MIEĆ WPŁYW NA BEZPIECZEŃSTWO INFORMACJI NIEJAWNYCH W URZĘDZIE GMINY W SANTOKU

opracowano zgodnie z rozporządzeniem
Rady Ministrów z dnia 29 maja 2012r. w sprawie środków bezpieczeństwa fizycznego stosowanych do zabezpieczania informacji niejawnych.
(Dz.U. nr. 115, poz.683, z dnia 19 czerwca 2012 r.)

KLAUZULA TAJNOŚCI PRZETWARZANYCH INFORMACJI NIEJAWNYCH

w Urzędzie Gminy w Santoku

L.p.	KLAUZULA TAJNOŚCI	TAK/NIE
1.	ściśle tajne	**NIE**
2.	tajne	**NIE**
3.	poufne	**NIE**
4.	zastrzeżone	**TAK**

L.p.	OCENA ISTOTNOŚCI CZYNNIKA	PRZYZNANO*
1.	Bardzo istotny (8pkt.)	
2.	Istotny (4 pkt.)	
3.	Mało istotny (1 pkt.)	1

UZASADNIENIE:

W Urzędzie Gminy w Santoku przetwarzane są dokumenty niejawne o klauzuli „zastrzeżone". Ww. dokumenty przetwarzane są wyłącznie w pomieszczeniu Kancelarii Materiałów Niejawnych, które zlokalizowane jest w pokoju nr 24 na pierwszym piętrze, przez osobę posiadającą poświadczenie bezpieczeństwa lub upoważnienie oraz odpowiednie przeszkolenie. Liczba dokumentów opatrzonych ww. klauzulą jest niewielka. W skali roku ilość wytworzonych dokumentów uzależniona jest od wniosków napływających np. w sprawie: świadczeń, planów obronnych, obrony cywilnej. Z uwagi na powyższe przyznano: 1 pkt.

LICZBA MATERIAŁÓW NIEJAWNYCH

w Urzędzie Gminy w Santoku

L.p.	KLAUZULA TAJNOŚCI	LICZBA MATERIAŁÓW NIEJAWNYCH
1.	ściśle tajne	0
2.	tajne	0
3.	poufne	0
4.	zastrzeżone	271

L.p.	OCENA ISTOTNOŚCI CZYNNIKA	PRZYZNANO
1.	Bardzo istotny (8pkt.)	
2.	Istotny (4 pkt.)	
3.	Mało istotny (1 pkt.)	1 pkt.

UZASADNIENIE:

W Urzędzie Gminy w Santoku przetwarzane są dokumenty niejawne o klauzuli „zastrzeżone". Ww. dokumenty przetwarzane są wyłącznie w pomieszczeniu Kancelarii Materiałów Niejawnych, które zlokalizowane jest w pokoju nr 24 na pierwszym piętrze, przez osobę posiadającą poświadczenie bezpieczeństwa lub upoważnienie oraz odpowiednie przeszkolenie. W skali roku ilość wytworzonych dokumentów uzależniona jest od wniosków napływających np. w sprawie: świadczeń, planów obronnych, obrony cywilnej.

Ilość dokumentów o klauzuli tajności zastrzeżone jest nieznaczny więc celowe jest wybór czynnika jako mało istotny.

Z uwagi na powyższe przyznano: 1 pkt.

POSTAĆ INFORMACJI NIEJAWNYCH

w Urzędzie Gminy w Santoku

L.p.	POSTAĆ INFORMACJI NIEJAWNYCH	TAK / NIE
1.	Dokumenty nielektroniczne	TAK
2.	Dokumenty elektroniczne	NIE
3.	Inne: nagranie dźwiękowe, obrazem itp.	NIE

L.p.	OCENA ISTOTNOŚCI CZYNNIKA	PRZYZNANO
1.	Bardzo istotny (8pkt.)	
2.	Istotny (4 pkt.)	
3.	Mało istotny (1 pkt.)	1 pkt.

UZASADNIENIE:

W Urzędzie Gminy w Santoku przetwarzane są dokumenty niejawne o klauzuli „zastrzeżone". Ww. dokumenty przetwarzane są wyłącznie w pomieszczeniu Kancelarii Materiałów Niejawnych, które zlokalizowane jest w pokoju nr 24 na pierwszym piętrze, przez osobę posiadającą poświadczenie bezpieczeństwa lub upoważnienie oraz odpowiednie przeszkolenie.

Urząd nie posiada akredytowanego systemu teleinformatycznego do przetwarzania informacji niejawnych. Dokumenty mają tylko postać papierową.

Z uwagi na powyższe przyznano: 1 pkt.

LICZBA OSÓB

mających lub mogących mieć dostęp do informacji niejawnych
w Urzędzie Gminy w Santoku

L.p.	KLAUZULA TAJNOŚCI	LICZBA OSÓB
1.	ściśle tajne	0
2.	tajne	0
3.	poufne	3
4.	zastrzeżone	5

L.p.	OCENA ISTOTNOŚCI CZYNNIKA	PRZYZNANO
1.	Bardzo istotny (8pkt.)	
2.	Istotny (4 pkt.)	
3.	Mało istotny (1 pkt.)	1

UZASADNIENIE:

Oceniając istotność czynnika uwzględniono wszystkich pracowników Urzędu Gminy w Santoku, którzy posiadają upoważnienie do dostępu do informacji niejawnych z uwagi na realizację zadań z zakresu obronności, obrony cywilnej, zarządzania kryzysowego. Wśród nich są osoby zajmujące kierownicze stanowiska. Łącznie 8 osób. Zatrudnienie w Urzędzie Gminy wynosi średnio 34 osoby.

Ilość osób posiadających upoważnienie do dostępu do informacji niejawnych w Urzędzie Gminy nie oznacza, że osoby te zajmują się bieżącym przetwarzaniem dokumentów niejawnych. Osobą odpowiedzialną za bezpośrednią realizację zadań z zakresu obronności a jednocześnie prowadzącą Kancelarię Materiałów Niejawnych jest 1 pracownik posiadający poświadczenie bezpieczeństwa i niezbędne przeszkolenie.

Z uwagi na powyższe przyznano: 1 pkt.

LOKALIZACJA

Urzędu Gminy w Santoku

L.p.	Rodzaj zabudowy	Opis
1.	Budynek wolnostojący	Budynek położony jest na działce, która stanowi własność Gminy Santok. Budynek użyteczności publicznej przeznaczony na potrzeby administracji publicznej. Posiada 3 kondygnacje. W budynku znajdują się dwie klatki schodowe. Dane charakterystyczne budynku: – pow. Użytkowa: 1054,59m^2 – kubatura: 3070,62 m^3 Budynek oddany do użytku w 1920 r. Pokryty jest dachem wielospadowym, pokrytym dachówką (karpiówką). Jedna ściana budynku przylega do innego budynku. Obok budynku znajdują się niewielkie ogólnodostępne parkingi, z których korzystają również pracownicy urzędu. Budynek nie sąsiaduje z obiektami przedstawicielstw i podmiotów zagranicznych, hotelami, obiektami sportowymi, zakładami przemysłowymi i instalacjami stanowiącymi zagrożenie dla życia lub zdrowia.

L.p.	OCENA ISTOTNOŚCI CZYNNIKA	PRZYZNANO
1.	Bardzo istotny (8pkt.)	
2.	Istotny (4 pkt.)	
3.	Mało istotny (1 pkt.)	1 pkt.

UZASADNIENIE:

Układ i lokalizacja budynku daje podstawę do określenia czynnika jako mało istotny.

Z uwagi na powyższe przyznano: 1 pkt

DOSTĘP DO BUDYNKU

osób niebędących pracownikami
Urzędu Gminy w Santoku

L.p.	ZAGADNIENIE	OPIS
1.	Osoby jakiej jednostki/*nazwa jednostki*/	W godzinach pracy urzędu dostęp do budynku posiadają pracownicy innych jednostek organizacyjnych Gminy Santok, kierownicy jednostek gminnych, radni, posłowie, goście.
2.	Szacunkowa liczba tych osób	35 osób na tydzień
3.	Interesanci	145 osób/tydzień (mieszkańcy gminy)

L.p.	OCENA ISTOTNOŚCI CZYNNIKA	PRZYZNANO
1.	Bardzo istotny (8pkt.)	
2.	Istotny (4 pkt.)	4 pkt.
3.	Mało istotny (1 pkt.)	

UZASADNIENIE:

Swobodna możliwość przemieszczania się po korytarzach budynku Urzędu Gminy ma istotny wpływ na wzrost oceny istotności tego czynnika. Budynek nie posiada systemu kontroli dostępu. Po godzinach urzędowania uruchamiany jest w system sygnalizacji włamania i napadu. Czujniki ruchu rozmieszczone są na terenie budynku. Działa system monitoringu wizyjnego wokół budynku.
Z uwagi na powyższe przyznano: 4 pkt

INNE CZYNNIKI

Urząd Gminy w Santoku

L.p.	CZYNNIK	TAK / NIE
1.	Działanie obcych służb specjalnych	TAK
2.	Sabotaż, zamach terrorystyczny	TAK
3.	Kradzież lub inna działalność przestępcza	TAK
4.	Pożar, działanie sił przyrody (np. powódź)	TAK

L.p.	OCENA ISTOTNOŚCI CZYNNIKA	PRZYZNANO
1.	Bardzo istotny (8pkt.)	
2.	Istotny (4 pkt.)	
3.	Mało istotny (1 pkt.)	1 pkt

UZASADNIENIE:

Obserwacja współczesnych zjawisk przyrodniczych oraz patologii społecznej w Polsce wymieniona jest w ujętej tabeli. Zjawiska pogodowe nie będą powodowały potencjalnych strat z uwagi na możliwość odtworzenia informacji z kopii. Wielopoziomowy system zabezpieczeń uniemożliwi kradzież materiałów niejawnych.
Z uwagi na powyższe czynnik określono jako mało istotny.
Z uwagi na powyższe przyznano: 1 pkt.

TABELA OKREŚLAJĄCA POZIOM ZAGROŻEŃ
w Urzędzie Gminy w Santoku

L.P.	CZYNNIK	OCENA ISTOTNOŚCI CZYNNIKA		
		BARDZO ISTOTNY (8 pkt.)	ISTOTNY (4 pkt.)	MAŁO ISTOTNY (1 pkt.)
1.	Klauzula tajności przetwarzanych informacji niejawnych			**1**
2.	Liczba materiałów niejawnych			**1**
3.	Postać informacji niejawnych			**1**
4.	Liczba osób			**1**
5.	Lokalizacja			**1**
6.	Dostęp osób do budynku		**4**	
7.	Inne czynniki			**1**
SUMA PUNKTÓW			**4**	**6**
RAZEM – *wszystkie punkty*			**10**	

TABELA DO OKREŚLENIA POZIOMU ZAGROŻEŃ

POZIOM ZAGROŻEŃ		
NISKI	ŚREDNI	WYSOKI
7 pkt – 16 pkt	17 pkt – 32 pkt	powyżej 32 pkt

W wyniku przeprowadzonej analizy poszczególnych czynników ostateczny poziom zagrożeń mających lub mogących mieć wpływ na bezpieczeństwo informacji niejawnych w Urzędzie Gminy w Santoku określono jako: niski.

Dla **NISKIEGO** poziomu zagrożeń i najwyższej klauzuli informacji niejawnych **„zastrzeżone"**- minimalna liczba punktów do osiągnięcia, wskazana w tabeli „PODSTAWOWE WYMAGANIA BEZPIECZEŃSTWA FIZYCZNEGO" wynosi 2.

Poziom Zagrożeń - ZASTRZEŻONE

	Niski	**Średni**	**Wysoki**
ZASTRZEŻONE			
Obowiązkowo: kategorie K1+K2+K3	2	**2**	2
Dodatkowo: kategoria K4, K5 lub K6	-	**1**	2
Łącznie suma punktów		**3**	4

W przypadku niskiego poziomu zagrożeń nie są wymagane dodatkowe zabezpieczenia z kategorii K4, K5 lub K6. W analizie uwzględniono jednak kategorię K4, jako zabezpieczenie dodatkowe.

DOBÓR ŚRODKÓW BEZPIECZEŃSTWA FIZYCZNEGO

KATEGORIA K1: Szafy do przechowywania informacji niejawnych,
Środek bezpieczeństwa K1S1 - Konstrukcja szafy: typ 1
K1S1= 1 pkt.
Środek bezpieczeństwa K1S2 - Zamek do szafy: typ 2
K1S2=2 pkt.
Liczba punktów za kategorię stanowiącą iloczyn liczby punktów za powyższe środki bezpieczeństwa (K1= K1S1x K1S2) = **2 pkt.**

KATEGRIA K2: Pomieszczenia
Środek bezpieczeństwa K2S1 - konstrukcja pomieszczenia : typ 1
K2S1= 1 pkt.
Środek bezpieczeństwa K2S2 - zamek do drzwi pomieszczenia: typ 1
K2S2= 1 pkt.
Liczba punktów za kategorię stanowiącą iloczyn liczby punktów za powyższe środki bezpieczeństwa (K2=K2S1x K2S2) = **1 pkt.**

KATEGORIA K3: Budynki : typ 1
Liczba punktów za kategorię K3=**1 pkt**.

ŁĄCZNA LICZBA PUNKTÓW ZA KATEGORIE **K1+K2+K3 = 4 pkt** - jest większa od wymaganej do osiągnięcia (2)

KATEGORIA K4: Kontrola dostępu
Środek bezpieczeństwa K4S1 – systemy kontroli dostępu: typ 1
K4S1=1 pkt.
Środek bezpieczeństwa K4S2 - Kontrola osób nieposiadających stałego upoważnienia do wejścia na obszar jednostki organizacyjnej (interesantów)
K4S2 = 0pkt.
Liczba punktów za kategorię stanowiącą sumę liczby punktów za oba powyższe środki bezpieczeństwa (K4= K4S1+K4S2)= **1 pkt.**

ŁĄCZNA LICZBA PUNKTÓW ZA KATEGORIE **K1+K2+K3+K4= 5** – jest większa od wymaganej do osiągnięcia (2) - w związku z tym nie jest konieczne stosowanie dodatkowych środków bezpieczeństwa z kategorii K5 oraz K6.

TABELA WYZNACZANIA PUNKTACJI ZA ZASTOSOWANE ŚRODKI BEZPIECZEŃSTWA FIZYCZNEGO

ŚRODEK BEZPIECZEŃSTWA	PUNKTACJA
KATEGORIA K1: SZAFY DO PRZECHOWYWANIA INFORMACJI NIEJAWNYCH	
Środek bezpieczeństwa K1S1- Konstrukcja szafy	
Liczba punktów za środek bezpieczeństwa K1S1	**1**
Środek bezpieczeństwa K1S2 – Zamek do szafy	
Liczba punktów za środek bezpieczeństwa K1S2	**2**
Liczba punktów za kategorię K1 stanowiąca iloczyn punktów za oba powyższe środki bezpieczeństwa (K1=K1S1xK1S2)	**2**
KATEGORIA K2: POMIESZCZENIA	
Środek bezpieczeństwa K2S1 – Konstrukcja pomieszczenia	
Liczba punktów za środek bezpieczeństwa K2S1	**1**
Środek bezpieczeństwa K2S2- Zamek do drzwi pomieszczenia	
Liczba punktów za środek bezpieczeństwa K2S2	**1**
Liczba punktów za kategorię K2 stanowiącą iloczyn liczby punktów za oba powyższe środki bezpieczeństwa (K2=K2S1xK2S2)	**1**
KATEGORIA K3 – BUDYNKI	
Liczba punktów za kategorię K3	**1**
KATEGORIA K4: KONTROLA DOSTĘPU	
Środek bezpieczeństwa K4S1 – Systemy kontroli dostępu	
Liczba punktów za środek bezpieczeństwa K4S1	**1**
Środek bezpieczeństwa K4S2 – Kontrola gości	
Liczba punktów za środek bezpieczeństwa K4S2	**0**
Liczba punktów za kategorię K4 stanowiącą sumę liczby punktów za oba powyższe środki bezpieczeństwa (K4= K4S1+K4S2)	**1**
Ogólna liczba punktów stanowiąca sumę punktów za wszystkie kategorie PUNKTY = K1+K2+K3+K4	**5**

Ogólna liczba punktów stanowiąca sumę punktów za wszystkie kategorie K1+K2+K3+K4=5

– jest większa od wymaganej do osiągnięcia (2) - w związku z tym nie jest konieczne stosowanie dodatkowych środków bezpieczeństwa z kategorii K5 i K6.

Przy określaniu zabezpieczeń zastosowanych do ochrony informacji niejawnych rozpatrywano kategorie obowiązkowe.

Zastosowane zabezpieczenia pozwalają na właściwą ochronę fizyczną informacji i nie ma potrzeby stosowania dodatkowych zabezpieczeń.

Zapewnienie poufności, dostępności i integralności informacji niejawnych osiągnięto przez:

- zapewnienie właściwego przetwarzania informacji niejawnych,
- umożliwienie zróżnicowania dostępu do informacji niejawnych dla pracowników zgodnie z posiadanymi przez nich uprawnieniami oraz uzasadnioną potrzebą dostępu do informacji niejawnych,
- wykrywanie, udaremnianie lub powstrzymywanie nieuprawnionych działań,
- uniemożliwianie lub opóźnianie wtargnięcia osób nieuprawnionych do pomieszczenia lub obszaru, w którym przetwarzane są informacje niejawne.

Środki bezpieczeństwa fizycznego stosuje się we wszystkich pomieszczeniach, w których przetwarzane są informacje niejawne.

W wyniku przeprowadzonej analizy w celu określenia poziomu zagrożeń, zastosowano odpowiednią kombinację następujących środków bezpieczeństwa fizycznego:

- bariery fizyczne – środki chroniące granice miejsca, w których przetwarzane są informacje niejawne, a w szczególności ściany drzwi i okna,
- szafy i zamki – stosowane do przechowywania informacji niejawnych lub zabezpieczające te informacje przed nieuprawnionym dostępem,
- system kontroli dostępu – obejmujący rozwiązanie organizacyjne, stosowany w celu zagwarantowania uzyskiwania dostępu do pomieszczenia lub obszaru, w którym przetwarzane są informacje niejawne, wyłącznie przez osoby posiadające odpowiednie uprawnienia.

Ponadto, utworzono strefę ochronną III – obejmującą pomieszczenie, w którym informacje niejawne o klauzuli „zastrzeżone" są przetwarzane w taki sposób, że wstęp do tego pomieszczenia nie umożliwia uzyskania bezpośredniego dostępu do tych informacji.

Załącznik nr 4 do Zarządzenia nr 37/2023 z dnia 15.09.2023r.

URZĄD GMINY W SANTOKU

SZACOWANIE RYZYKA
DLA BEZPIECZEŃSTWA INFORMACJI NIEJAWNYCH, PRZETWARZANYCH W URZĘDZIE GMINY W SANTOKU

OPRACOWAŁ:
Pełnomocnik ds. Ochrony Informacji Niejawnych
Krzysztof Kinal

SANTOK

Wrzesień 2023

Spis Treści

Wstęp

Proces analizy ryzyka polega na identyfikacji ryzyk, tzn. prawdopodobieństwa wystąpienia określonych zagrożeń wykorzystujących podatność systemu, określenia ich wielkości i wpływu na bezpieczeństwo systemu oraz opisaniu obszarów wymagających zabezpieczenia i zastosowania środków ochrony.

I. Szacowanie ryzyka

1. Identyfikacja ryzyka

Proces oszacowania ryzyka został opracowany w oparciu o macierz występujących zagrożeń dla poufności, dostępności i integralności dla zidentyfikowanych zasobów systemu. W podejściu tym ryzyko szacowane jest jakościowo w oparciu o wybrany poziom wymagań bezpieczeństwa. W celu scharakteryzowania wybranego poziomu posłużono się skalą 10-cio stopniową.

W rzędach macierzy wyszczególniane są zasoby systemu podlegające ochronie. Kolumny przedstawiają ryzyka, jakie zagrażają integralności, poufności i dostępności tych zasobów. W poszczególne komórki macierzy wpisywane są rezultaty oszacowanych skutków utraty atrybutów bezpieczeństwa informacji, podatności zasobów na zidentyfikowane dla systemu zagrożenia i wyniki obliczonego dla każdego zasobu ryzyka.

2. Estymacja ryzyka

2.1. Szacowanie skutków utraty zasobów

a) zachowanie integralności

Przyjęto cztery poziomy wymagań dotyczących potrzeby zachowania integralności. Liczby z tych zakresów umożliwiają zróżnicowanie zasobów informacji mieszczących się w tej samej kategorii i odpowiadają skutkom, jakie może spowodować dane zagrożenie:

1. Niskie (1-3),
2. Średnie (4-7),
3. Wysokie (8-9),
4. Bezwzględne(10)

b) zachowanie poufności informacji

W zależności od klauzuli zasobów przyjęto:

1. Jawne (0),
2. Zastrzeżone (1-3),
3. Poufne (4-5),
4. Tajne (6-7),
5. Ściśle tajne (8-10).

c) zachowanie dostępności informacji

Przyjęto następujące przedziały wartości w odniesieniu do skutków:

1. niskie wymagania (1-3) - oznacza, że jeżeli informacje były niedostępne, nie miało to większego wpływu na zadania urzędu w większym przedziale czasu,
2. średnie wymagania (4-6) - oznacza, że niedostępność informacji może mieć znaczący wpływ i odzyskanie dostępności musi nastąpić w ciągu kilku dni,
3. wysokie wymagania (7-8) - oznacza, że niedostępność informacji może spowodować duże szkody w działalności urzędu i odzyskanie dostępności musi nastąpić w ciągu kilku godzin,
4. ekstremalne wymagania (9) - oznacza, że działalność urzędu zostanie sparaliżowana i odzyskanie dostępu musi nastąpić w ciągu kilku minut,
5. absolutne wymagania (10) - oznacza, że nie dopuszcza się utraty dostępności informacji.

2.2. Oszacowanie podatności zasobów

Dla każdego zidentyfikowanego zagrożenia oszacowano podatność każdej kategorii zasobów. Przy szacowaniu wzięte pod uwagę zostało prawdopodobieństwo wystąpienia zagrożenia i podatność systemu, która umożliwi powstanie szkody w systemie.

Przyjęto następujące poziomy podatności i odpowiadające im zakresy wartości:

1. Brak (0),
2. Niski poziom (1-4),
3. Średni poziom (5-7),
4. Wysoki poziom (8-9),
5. Ekstremalny poziom (10).

2.3. Oszacowanie ryzyka

Wynikiem szacowania ryzyka jest wartość ryzyka dla każdej kategorii zasobów systemu i zagrożenia, otrzymana poprzez pomnożenie wartości odpowiadających sobie skutków i podatności. Przyjęto następujące poziomy wielkości ryzyka dla obliczonych wartości liczbowych ryzyka.

1. Niski (1-20),
2. Średni (21-60),
3. Wysoki (61-80),
4. Maksymalny (81-100).

Kolorem czerwonym zaznaczono te obszary, które cechują się największym ryzykiem wystąpienia zagrożenia utraty atrybutów bezpieczeństwa dla poszczególnych zasobów.

Większość strat spowodowana jest przez przypadkowe zdarzenia ze względu na wysokie prawdopodobieństwo ich wystąpienia, chociaż wpływ takiego zagrożenia jest ograniczony. Działania zamierzone mogą mieć groźniejsze skutki, ale cechuje je mniejsze prawdopodobieństwo i częstotliwość.

II. Ocena ryzyka

1 . Zasoby systemu

- Plan Operacyjny Funkcjonowania Urzędu Gminy w Santoku w warunkach zewnętrznego zagrożenia bezpieczeństwa państwa i w czasie wojny,
- dokumentacja głównego stanowiska kierowania,
- regulamin organizacyjny Urzędu Gminy na czas „W",
- dokumentacja przemieszczenia Urzędu do zapasowego miejsca pracy, organizacja zapasowego miejsca pracy Wójta Gminy.

2. Identyfikacja zagrożeń

2.1 Zagrożenia przypadkowe:

W celu późniejszego wypełnienia macierzy zagrożeniom zostały przypisane symbole (ZG1 do ZG17).

Za potencjalne zagrożenia przypadkowe systemu należy uznać:

- błędy, pomyłki użytkowników (ZG1),
- pozostawianie dokumentów (ZG3),
- niezamykanie pomieszczeń i/lub sejfów (ZG4),
- ujawnienie informacji (ZG5),
- wynoszenie materiałów niejawnych poza strefę (ZG6),
- zmiana zawartości zgromadzonych danych (ZG7),
- usunięcie części danych/dokumentów (ZG8),
- fizyczne zniszczenie zasobów (ZG9),
- awarie sprzętu, instalacji elektrycznej i CO (ZG10),
- klęski żywiołowe (ZG11).

Potencjalnymi sprawcami wyżej wymienionych zagrożeń (poza „siłami wyższymi") mogą być ludzie popełniający niezamierzone błędy wskutek nieświadomości, braku umiejętności lub niestaranności i nieprzestrzegania obowiązujących procedur.

2.2. Zagrożenia zamierzone – celowe

Do potencjalnych zagrożeń celowych systemu należy zaliczyć:

- niezamykanie pomieszczeń i/lub sejfów (ZG4),
- pozostawianie dokumentów (ZG3),
- przełamanie haseł dostępu systemu alarmowego(ZG12),
- nieuprawnione przeglądanie zasobów (ZG13),
- usunięcie części danych/dokumentów (ZG8),
- fizyczne zniszczenie zasobów (ZG9),
- podgląd edytowanych tekstów (ZG14),
- podsłuch podczas dyktowania treści dokumentów (ZG15),

- ujawnienie informacji (ZG5),
- wynoszenie materiałów niejawnych poza strefę (ZG6),
- awarie sprzętu, instalacji elektrycznej i CO (ZG10),
- kradzież sprzętu (ZG16),
- dywersja i terroryzm (ZG17).

Potencjalnymi sprawcami wyżej wymienionych zagrożeń mogą być:

- osoby (organizacje) spoza Urzędu Gminy w Santoku, zainteresowane pozyskaniem istotnych dla nich informacji,
- użytkownicy systemu powodowani ciekawością,
- użytkownicy systemu – niezadowolony personel „na złość przełożonym lub kolegom",
- użytkownicy systemu zwerbowani do współpracy z organizacjami (wyspecjalizowanymi służbami),
- personel techniczny mający dostęp do systemu, czyli ludzie podejmujący zamierzone, zaplanowane działania z zamiarem osiągnięcia określonych korzyści.

3. Podatności

Podatność zdefiniowana jako słabość danego systemu wynikająca z błędów wewnętrznych lub błędów użytkownika. Podatności systemów zostały oszacowane dla niżej wymienionych zagrożeń.

Ze względu na charakter wykorzystania systemu – z reguły wytwarzanie (edycja) dokumentów (scharakteryzowanych w p. 1), danych istnieje małe zagrożenie utraty integralności i dostępności danych.

Potencjalnymi zagrożeniami dla integralności przetwarzanych w systemie informacji niejawnych są:

- błędy, pomyłki użytkowników (ZG1),
- awarie sprzętu, instalacji elektrycznej i CO (ZG10),
- kradzież sprzętu (ZG16),
- usunięcie części danych/dokumentów (ZG8),
- fizyczne zniszczenie zasobów (ZG9),

- klęski żywiołowe (ZG11),
- dywersja i terroryzm (ZG17).

Potencjalnymi zagrożeniami dla poufności przetwarzanych w systemie informacji niejawnych są:
- błędy, pomyłki użytkowników (ZG1),
- niezamykanie pomieszczeń i/lub sejfów (ZG4),
- pozostawianie dokumentów (ZG3),
- wynoszenie materiałów niejawnych poza strefę (ZG6),
- ujawnienie informacji (ZG5),
- nieuprawnione przeglądanie zasobów (ZG13),
- przełamanie haseł dostępu systemu alarmowego (ZG12),
- podgląd edytowanych tekstów (ZG14),
- podsłuch podczas dyktowania treści dokumentów(ZG15).

Natomiast zagrożeniami dla dostępności przetwarzanych w systemie informacji niejawnych są:
- błędy, pomyłki użytkowników (ZG1),
- usunięcie części danych (ZG8),
- zmiana zawartości zgromadzonych danych (ZG7),
- fizyczne zniszczenie zasobów (ZG9),
- przełamanie haseł dostępu systemu alarmowego (ZG12),
- awarie sprzętu, instalacji elektrycznej i CO (ZG10).

4. Dobór środków ochrony

System ochrony informacji niejawnych zabezpieczony jest zgodnie z dokumentacją określająca poziom zagrożeń związanych z nieuprawnionym dostępem do informacji niejawnych lub ich utratą, opracowaną na podstawie rozporządzenia Rady Ministrów z dnia 29 maja 2012 r. (Dz.U. z 2012 r., poz. 683) w sprawie środków bezpieczeństwa fizycznego stosowanych do zabezpieczenia informacji niejawnych.

5. Konsekwencje naruszenia celów bezpieczeństwa

Większość strat spowodowana może być przez przypadkowe zdarzenia ze względu na wysokie prawdopodobieństwo ich wystąpienia, chociaż wpływ takiego zagrożenia jest ograniczony. Działania zamierzone mogą mieć groźniejsze skutki, ale cechuje je mniejsze prawdopodobieństwo i częstotliwość. Największe ryzyko występuje dla zagrożenia utraty poufności przy zagrożeniu nieuprawnionego przeglądania zasobów (ZG13). Kolejnymi zagrożeniami zidentyfikowanymi w procesie szacowania ryzyka mogą okazać się przełamanie haseł dostępu, awaria instalacji elektrycznej i CO (ZG10). Podatność systemu na występujące zagrożenia jest minimalna i w praktyce może w ogóle się nie wydarzyć.

5.1. Ocena stopnia ważności informacji.

a) utrata poufności

Najistotniejsze znaczenie dla Urzędu Gminy w Santoku będzie miała poufność przetwarzanych informacji.

Utrata poufności tych informacji może spowodować najdotkliwsze skutki.

b) utrata integralności

Integralność przetwarzanych informacji ma nieco mniejsze znaczenie ze względu na to, że postacią finalną jest dokument papierowy, zarejestrowany oraz przechowywany w strefie bezpieczeństwa.

c) utrata dostępności

Dostępność przetwarzanych informacji ma najmniejsze znaczenie ze względu na to, że dostęp do nich nie jest krytyczny. Utrata dostępności spowoduje zatem najmniejsze straty.

5.2. Ryzyko szczątkowe.

Na podstawie analizy zagrożeń i podatności systemu oraz zdefiniowanych środków zabezpieczających, które będą wdrożone dla zminimalizowania występującego ryzyka uznano, że osiągnięty zostanie wymagany poziom bezpieczeństwa.

Pozostałe ryzyko, związane z brakiem możliwości monitorowania i kontroli pracowników w czasie pracy stanowi zagrożenie dla poufności przetwarzanych informacji - jest ono znane i akceptowalne – zakłada się odpowiedzialne i świadome działanie osób mających dostęp do informacji niejawnych, postępowanie zgodnie z przepisami prawa. Podatność systemu na pozostałe zagrożenia nieuwzględnione w macierzy oszacowania ryzyka oszacowano na minimalne niepowodujące szkody dla systemu ochrony informacji niejawnych.

Kierownik jednostki akceptuje wyniki procesu szacowania ryzyka, zna oraz akceptuje pozostałe ryzyko szczątkowe.

6. Macierz oszacowania ryzyka

Zasoby Systemu		Szacowanie	Zagrożenia																						
			Poufność									Integralność							Dostępność						
Rodzaj Informacji	Klauzula		ZG1	ZG4	ZG3	ZG6	ZG5	ZG13	ZG12	ZG14	ZG15	ZG1	ZG10	ZG16	ZG8	ZG9	ZG11	ZG17	ZG1	ZG8	ZG7	ZG9	ZG12	ZG10
Plan operacyjny funkcjonowania UG w warunkach zew. zagr. bezp. państwa i w czasie wojny	Zastrzeżone	skutki	4	4	4	4	4	4	5	4	4	3	1	1	2	1	1	1	1	1	1	1	1	1
		podatność	1	1	1	1	1	2	1	1	1	1	2	1	1	1	1	1	1	1	1	1	1	2
		ryzyko	4	4	4	4	4	8	5	4	4	3	2	1	2	1	1	1	1	1	1	1	1	2
Dokumentacja głównego stanowiska kierowania	Zastrzeżone	skutki	1	3	1	3	3	4	2	2	2	3	1	1	2	1	1	1	1	1	1	1	1	1
		podatność	1	1	2	1	1	1	1	1	1	1	2	1	1	1	1	1	2	1	1	1	1	2
		ryzyko	1	3	2	3	3	4	2	2	2	3	2	1	2	1	1	1	2	1	1	1	1	2
Regulamin organizacyjny UG na czas "W"	Zastrzeżone	skutki	1	3	1	3	3	4	2	2	2	3	1	1	2	1	1	1	1	1	1	1	1	1
		podatność	1	1	2	1	1	1	1	1	1	1	2	1	1	1	1	1	2	1	1	1	1	2
		ryzyko	1	3	2	3	3	4	2	2	2	3	2	1	2	1	1	1	2	1	1	1	1	2
Dokumentacja przemieszczenia urzędu do zapasowego miejsca pracy, organizacja zapasowego miejsca pracy	Zastrzeżone	skutki	1	3	1	3	3	3	2	2	2	3	1	1	2	1	1	1	1	1	1	1	1	1
		podatność	1	1	2	1	1	1	1	1	1	1	2	1	1	1	1	1	2	1	1	1	1	2
		ryzyko	1	3	2	3	3	3	2	2	2	3	2	1	2	1	1	1	2	1	1	1	1	2

Załącznik nr 4 do planu ochrony

REJESTR WEJŚĆ/WYJŚĆ DO STREFY BEZPIECZEŃSTWA

lp	Imię i nazwisko	Data	Godzina		Podpis	Uwagi
			wejście	wyjście		
1	2	3	4	5	6	7