Zarządzenie nr RO.120.2.2023
Wójta Gminy Siennica – Kierownika Urzędu
z dnia 11 stycznia 2023 roku
w sprawie wprowadzenia Planu Ochrony Informacji Niejawnych
w Urzędzie Gminy w Siennicy

Na podstawie art. 15 ust. 2 w związku z art. 14 ust. 1, art. 52 ust. 1 ustawy z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych (Dz. U. z 2019 r. poz. 742), zarządza się co następuje:

§ 1.

W celu zapewnienia ochrony informacji niejawnych wprowadza się „Plan Ochrony Informacji Niejawnych w Urzędzie Gminy w Siennicy" w brzmieniu załącznika nr 1 do niniejszego zarządzenia.

§ 2.

Wykonanie zarządzenia powierza się Pełnomocnikowi ds. Ochrony Informacji Niejawnych.

§ 3.

Zarządzenie wchodzi w życie z dniem podpisania.

Załącznik nr 1 do Zarządzenia nr RO.120.2.2023 z dnia 11 stycznia 2023 roku

Plan Ochrony Informacji Niejawnych w Urzędzie Gminy w Siennicy

Opracował:

Małgorzata Kobza

Pełnomocnik ds. Ochrony Informacji Niejawnych

Zatwierdził:

Stanisław Duszczyk

Wójt Gminy Siennica

Spis treści

1. Wstęp

W Urzędzie Gminy w Siennicy 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 – „Bezpiecznego Stanowiska".

1.1. Podstawy prawne

Plan ochrony informacji niejawnych Urzędu Gminy w Siennicy sporządzony został na podstawie art. 15 ust. 1 pkt 5 ustawy z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych (tj. Dz. U. z 2019 r. poz. 742 ze zm.) z uwzględnieniem zapisów wynikających z aktów wykonawczych do przywołanej ustawy:

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

1) Rozporządzenia Prezesa Rady Ministrów z dnia 22 grudnia 2011 r. w sprawie sposobu oznaczania materiałów i umieszczania na nich klauzul tajności (tj. Dz. U. z 2011 Nr 288, poz. 1692 ze zm.),
2) Rozporządzenia Prezesa Rady Ministrów z dnia 7 grudnia 2011 r. w sprawie nadawania, przyjmowania, przewożenia, wydawania i ochrony materiałów zawierających informacje niejawne (tj. Dz. U. z 2011 r. Nr 271, poz. 1603 ze zm.),
3) Rozporządzenie Prezesa Rady Ministrów z dnia 28 grudnia 2010 r. w sprawie wzorów poświadczeń bezpieczeństwa (tj. Dz. U. z 2015 r. poz. 220 ze zm.),
4) Rozporządzenia Prezesa Rady Ministrów z dnia 28 grudnia 2010 r. w sprawie wzoru decyzji o cofnięciu poświadczenia bezpieczeństwa (tj. Dz. U. z 2010 r. Nr 258, poz. 1754 ze zm.),
5) Rozporządzenia Prezesa Rady Ministrów z dnia 28 grudnia 2010 r. w sprawie wzoru decyzji o odmowie wydania poświadczenia bezpieczeństwa (tj. Dz. U. z 2010 r. Nr 258, poz. 1753 ze zm.),
6) Rozporządzenia Prezesa Rady Ministrów z dnia 20 lipca 2011 r. w sprawie podstawowych wymagań bezpieczeństwa teleinformatycznego (tj. Dz. U. z 2011 r. Nr 159, poz. 948 ze zm.).

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 (tj. Dz. U. z 2020 r. poz. 344 ze zm.) 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 (tj. 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;
- **Bezpieczne Stanowisko** - to stanowisko komputerowe służące do opracowywania dokumentów niejawnych o klauzuli „zastrzeżone";
- **Jednostka organizacyjna** – Urząd Gminy w Siennicy;
- **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.

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

1.1.Opis budynku i jego sąsiedztwo

Przetwarzanie informacji niejawnych w Urzędzie Gminy w Siennicy realizowane jest w obiekcie Urzędu przy ul. Mińskiej 33, 05-332 Siennica.

W otoczeniu budynków 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. Teren wokół doświetlany lampami ulicznymi.

Budynek Urzędu wykonany z pełnych materiałów budowlanych, dwukondygnacyjny. Dach w konstrukcji drewnianej, wielospadowy, kryty blachodachówką. Do obiektu prowadzą 3 wejścia zabezpieczane drzwiami niecertyfikowanymi z profili aluminiowych z przeszkleniami, zamykanymi na zamki z wkładką patentową (po jednym zamku). Drzwi obiektu otwierają upoważnieni przez Wójta pracownicy Urzędu. Osoby te są zobowiązane uzbrajać i rozbrajać system alarmowy obiektu (indywidualny kod dla każdego użytkownik). Okna z profili aluminiowych, niecertyfikowane i nieokratowane.

W obiekcie uruchomione są elektroniczne systemy:

- System alarmowy – wyposażony w czujki ruchu obejmujące swoim zasięgiem ciągi komunikacyjne obiektu oraz pomieszczenia biurowe. Sygnały alarmowe przekazywane są do firmy ochrony osób i mienia „SERIS Konsalnet Holding S.A.", która na podstawie zawartej umowy jest zobowiązana do wysłania grupy interwencyjnej w czasie:
  - w godz. 6.00 – 20.00 do 12 min. od otrzymania sygnału alarmowego,
  - w godz. 20.00 – 6.00 do 8 minut od otrzymania sygnału alarmowego.
- System monitoringu wizyjnego – wyposażony łącznie w 27 kamer wewnętrznych oraz zewnętrznych, w polu widzenia których znajduje się teren wokół Urzędu wraz przyległymi parkingami, wejścia do obiektu oraz ciągi komunikacyjne Urzędu (hole, korytarze, klatki schodowe). System umożliwia rejestrację wizerunku osób wchodzących do obiektu oraz poruszających się po jego terenie. Materiał zapisywany jest na rejestratorach zlokalizowanych w serwerowni Urzędu i jest przechowywany przez co najmniej 14 dni (zapis w pętli). Obsługę systemu – w tym zarejestrowanego materiału – zapewnia upoważniony przez Wójta pracownik Urzędu.

W obiekcie funkcjonuje Gminna Biblioteka, podmiot podległy pod Wójta Gminy, do którego prowadzi osobne wejście. Biblioteka nie posiada wydzielonej strefy systemu alarmowego, objęta zasięgiem kamer systemu monitoringu wizyjnego Urzędu.

1.2.Opis pomieszczenia, w którym przetwarzane są informacje niejawne

Pomieszczenia przetwarzania informacji niejawnych:

- Pomieszczenie sekretariatu Wójta – w którym odbierane, otwierane, rejestrowane i przekazywane do dekretacji Wójta są przesyłki niejawne, pomieszczenie „Sekretariat",

położone na piętrze Urzędu, zamykane drzwiami (drewniane pełne biurowe), zamykane na zamek z wkładką bębenkową, całość niecertyfikowana.

- Pomieszczenie Bezpiecznego Stanowiska – pomieszczenie techniczne „F" – usytuowane na piętrze wydzielone pomieszczenie o ścianach wykonanych z pełnych materiałów budowlanych, bez okien. Drzwi wejściowe do pomieszczenia pełne biurowe, zamykane na zamek z wkładką bębenkową, niecertyfikowane. Pomieszczenie nie jest stałym miejscem pracy żadnego pracownika – jest to pomieszczenie dedykowane wyłącznie pod system TI Bezpieczne Stanowisko.

2. 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 wymienionych pomieszczeń odbywa się w formie elektronicznej.

2.1.Osoby upoważnione

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 sekretariatu stanowią część kompletu kluczy do otwierania Urzędu i pozostają w dyspozycji pracowników wybranych uprawnionych pracowników.

Klucze do pomieszczenia technicznego F, będącego pomieszczeniem Bezpiecznego Stanowiska wydaje pracownik sekretariatu Urzędu na podstawie zatwierdzonej przez Wójta listy osób uprawnionych (listy użytkowników systemu). Fakt ten podlega odnotowaniu w odpowiednim rejestrze wydanych kluczy, zawierającego imię i nazwisko pobierającego, datę i godzinę pobrania oraz podpis pobierającego. W przypadku zdania klucza wiersz uzupełnia się o datę i godzinę zdania klucza oraz pracownik sekretariatu potwierdza fakt zdania własnym podpisem.

2.2.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 wejścia osób nieuprawnionych w podlega odnotowaniu w rejestrze wejść/wyjść osób obcych.

3. Określenie poziomu zagrożeń

3.1.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 2021 roku: 21 dokumentów.
3	Postać informacji niejawnych			1	W chwili sporządzenia niniejszego plany wyłącznie forma papierowa w niewielkich ilościach.
4	Liczba osób			1	W Urzędzie zatrudnionych jest obecnie osób 47 z czego poświadczenia bezpieczeństwa posiada 1 osoba (około 2 % zatrudnionych) i 8 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 czterema wejściami. Po godzinach pracy obiekt zamknięty i zabezpieczony systemem alarmowym z powiadomieniem do firmy ochrony osób i mienia.
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).

3.2.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)	3
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	**8**

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

4. Opis zastosowanych środków bezpieczeństwa fizycznego

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

- Utworzono pion ochrony (Zarządzenie Nr RO.120.1.2023 Wójta Gminy Siennica – Kierownika Urzędu z dnia 11 stycznia 2023 r.) w ramach którego wyznaczono/zatrudniono 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 Bezpiecznego Stanowiska 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 przetwarzającego informacje niejawne – „Bezpiecznego Stanowiska", 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 powiadomieniem firmy ochrony osób i mienia, z reakcją grupy interwencyjnej,
    - wprowadzono organizacyjną kontrolę dostępu do pomieszczeń przetwarzania informacji niejawnych,
    - w obiekcie funkcjonuje system monitoringu wizyjnego, rejestrującego wizerunek osób poruszających się wokół obiektu oraz wewnątrz obiektu,
    - 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 Bezpieczne Stanowisko.

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.

5. 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.

5.1.Zarządzanie kluczami do pomieszczenia

Klucze do użytku bieżącego pomieszczeń przetwarzania informacji niejawnych wydawane są na podstawie listy osób upoważnionych, zatwierdzonej przez kierownika jednostki organizacyjnej. Fakt wydania i przyjęcia klucza odnotowywany jest w odpowiednim rejestrze.

Klucze zapasowe do chronionych pomieszczeń pozostają w dyspozycji pracownika Sekretariatu 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.

5.2.Zarządzanie kluczami do szaf na materiały niejawne

Klucz do użytku bieżącego jest w dyspozycji pracownika użytkującego daną szafę, który posiada na stanie materiały niejawne i jest odpowiedzialny za ich należyte zabezpieczenie. Klucze zapasowe do szaf i mebli biurowych do przechowywania informacji niejawnych pozostają w dyspozycji pracownika Sekretariatu Gminy i wydawane są w sytuacji awaryjnej za zgodą lub na polecenie kierownika jednostki organizacyjnej – lub innej osoby uprawnionej do podjęcia merytorycznej decyzji.

W przypadku konieczności otwarcia indywidualnie użytkowanej szafy/szafy metalowej 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.

6. 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 bezpiecznego stanowiska, 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.

7. 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 w Siennicy 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 Bezpiecznego Stanowiska. 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.

8. 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).*

8.1.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 pkt. 4.

8.2.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 palnie wyrobów tytoniowych. Wyposażenie obiektu w urządzenia i instalacje gaśnicze (gaśnice, koce gaśnicze) jest adekwatne do instalacji użytkowanych w obiekcie (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 ternie obiektu (lub jego sąsiedztwie) należy postępować zgodnie z przyjętą w Urzędzie instrukcją przeciwpożarową, a w przypadku jej braku – dążyć do:

- Niezwłocznego zawiadomienia Straży Pożarnej o pożarze,
- Poinformowania innych osób w obiekcie o zagrożeniu (okrzykiem),
- 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.

8.3.Awaria techniczna skutkująca zalaniem pomieszczeń

W przypadku wystąpienia awarii technicznej skutkującej zalaniem wodą pomieszczeń należy:

- 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.
- 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).

8.4.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.

8.5.Awaria techniczna – system alarmowy

Niesprawność elektronicznego systemu alarmowego powodująca obniżenie poziomu zabezpieczeń jest natychmiast usuwana poprzez wyspecjalizowany serwis, któremu zleca się prace niezwłocznie po wykryciu usterki systemu.

8.6.Awaria techniczna – system monitoringu wizyjnego

Niesprawność elektronicznego systemu monitoringu wizyjnego powodująca obniżenie poziomu zabezpieczeń jest natychmiast usuwana poprzez wyspecjalizowany serwis, któremu zleca się prace niezwłocznie po wykryciu usterki systemu.

8.7.Włamanie – akty wandalizmu

Budynek urzędu chroniony jest systemem alarmowym z powiadomieniem firmy ochroniarskiej. W przypadku wyzwolenia alarmu w czasie od 8 do 12 minut 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.

8.8.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.

8.9.Awaria bezpiecznego stanowiska

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

8.10. 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, bezpiecznego stanowiska komputerowego na wyższe kondygnacje obiektu, tak, by np. w razie trwającej powodzi nie uległy zniszczeniu poprzez zalanie).

8.11. 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:

- nr 3 - szafa metalowa - osoba odpowiedzialna – Wiesław Ładusiak – tel. 25 747 43 35 przydzielono worek ewakuacyjny, który znajduje się w pomieszczeniu (szafa z materiałami niejawnymi)
- nr F - bezpieczne stanowisko komputerowe, osoba odpowiedzialna – Wiesław Ładusiak – tel. 25 747 43 35.

Do ewakuacji materiałów niejawnych przeznaczony jest samochód służbowy nr rej. WM 9993A, klucz i kontrolka w pomieszczeniu nr 11.

Do niszczenia materiałów niejawnych podlegających zniszczeniu w miejscu pracy „Z" przeznaczona jest niszczarka typu HSM Securio B34 klasy P4, znajdująca się w pomieszczeniu socjalnym.

Osoba odpowiedzialna za ewakuację materiałów niejawnych – Pełnomocnik ds. ochrony informacji niejawnych – Małgorzata Kobza - tel. 25 757 22 86.

W przypadku ewakuacji do zapasowego miejsca pracy (ZMP) ewakuowane materiały podlegają przewiezieniu do wyznaczonego obiektu, tj. Zespół Szkół im. Hipolity i Kazimierza Gnoińskich w Siennicy, ul. Mińska 38, 05-332 Siennica, w pozostałych przypadkach miejsce ewakuacji materiałów wskaże kierownik jednostki organizacyjnej lub inna uprawniona osoba, działająca w jego imieniu.