PROGRAM OCHRONY ZNANEGO NADAWCY PRZED AKTAMI BEZPRAWNEJ INGERENCJI

*Nazwa przedsiębiorcy*

**Lokalizacja Znanego Nadawcy:**

**Adres:**

**Nr dokumentu:**

**Nr egzemplarza:**

**Wydanie:**

**Zmiana:**

**Rejestr wprowadzonych zmian**

|  |  |  |
| --- | --- | --- |
| Zmiana nr | Data zmiany | Rozdziały |
| 1 |  |  |
| 2 |  |  |
| 3 |  |  |

SPIS TREŚCI

**1. Zagadnienia ogólne**

1.1 Cel programu ochrony

1.2 Dane teleadresowe przedsiębiorcy

1.3 Definicje.

1.4 Uregulowania prawne.

**2. Struktura organizacyjna.**

2.1 Zakres i charakter prowadzonej działalności.

2.2 Struktura organizacyjna przedsiębiorstwa.

2.3 Osoba odpowiedzialna ochronę.

**3. Środki ochrony.**

3.1 Ochrona fizyczna.

3.2 Produkcja.

3.3 Pakowanie.

3.4 Składowanie.

3.5 Wysyłka.

3.6 Przesyłka z innych źródeł.

3.7 Przewóz.

3.8 Cyberbezpieczeństwo.

**4. Wewnętrzna kontrola zgodności w zakresie ochrony lotnictwa cywilnego.**

4.1 Formy prowadzenia wewnętrznej kontroli zgodności.

4.2 Harmonogram wewnętrznej kontroli zgodności.

4.3 Dokumentacja wewnętrznej kontroli zgodności i sprawozdawczość.

**5. Wymagania dotyczące personelu.**

5.1 Sprawdzenie przeszłości.

5.2 Szkolenia.

5.3 Kultura ochrony oraz przeciwdziałanie zagrożeniom wewnętrznym.

**6. Zarządzanie kryzysowe.**

6.1 Procedury postępowania na wypadek nieuprawnionego dostępu do ładunków lotniczych
 lub poczty lotniczej.

6.2 Procedury postępowania na wypadek zagrożenia bombowego.

6.3 Informowanie o incydentach.

**7. Wykaz załączników.**

7.1 Deklaracja zobowiązań.

7.2 Formularz sprawdzenia przeszłości.

7.3 Lista przedmiotów zabronionych w ładunkach lotniczych lub poczcie lotniczej.

7.4 Plan obiektu z uwzględnieniem stref dostępu i punktów dostępu.

7.5 Kwestionariusz przyjęcia informacji o sytuacji kryzysowej.

7.6 Formularz zgłoszenia aktu bezprawnej ingerencji.

## Zagadnienia ogólne

##  Cel programu ochrony

Celem Programu ochrony *nazwa przedsiębiorcy* jest zapewnienie ochrony przed aktami bezprawnej ingerencji ładunkom przeznaczonym do transportu drogą lotniczą (zwanych dalej IPL lub identyfikowalnym ładunkiem lotniczym), które są wytwarzane, przechowywane i wysyłane z lokalizacji znanego nadawcy (*nazwa przedsiębiorcy)*.

Znany Nadawca:

1. Zgadza się na niezapowiedziane inspekcje przeprowadzane przez inspektorów upoważnionych przez Prezesa Urzędu Lotnictwa Cywilnego w celu monitorowania przedmiotowych norm. W przypadku stwierdzenia przez inspektorów poważnych uchybień w zakresie ochrony, może to skutkować cofnięciem statusu znanego dostawcy.
2. Przedstawi Prezesowi Urzędu Lotnictwa Cywilnego bezzwłocznie, jednak nie później niż w - terminie 10 dni roboczych, odpowiednie informacje szczegółowe, jeżeli:

- ogólna odpowiedzialność za ochronę zostanie przyznana innej osobie niż osoba wymieniona w pkt 2.2. i 2.4 programu ochrony

- w pomieszczeniach lub procedurach wystąpią inne zmiany, które mogą mieć znaczący wpływ na ochronę, oraz

- zaprzestanie działalności, przestanie zajmować się ładunkiem lotniczym/pocztą lotniczą lub przestanie spełniać wymogi odpowiedniego prawodawstwa Unii Europejskiej

c) Utrzyma normy stosowane w zakresie ochrony do następnej wizji lokalnej przeprowadzanej przez Prezesa Urzędu Lotnictwa Cywilnego lub do następnej inspekcji.

1. Przyjmuje na siebie pełną odpowiedzialność za złożoną deklarację.

##

##  Dane teleadresowe przedsiębiorcy

nazwa przedsiębiorcy:

adres:

nr KRS:

nr NIP:

nr certyfikatu AEO jeżeli dotyczy:

##  Definicje.

1. aktem bezprawnej ingerencji w lotnictwie cywilnym jest bezprawny i celowy akt polegający na:
2. użyciu w czasie lotu statku powietrznego przemocy wobec osoby znajdującej się na jego pokładzie, jeżeli akt ten może zagrozić bezpieczeństwu tego statku;
3. zniszczeniu statku powietrznego albo spowodowaniu jego uszkodzeń, które uniemożliwiają lot lub mogą stanowić zagrożenie bezpieczeństwa tego statku;
4. umieszczeniu na pokładzie statku powietrznego przedmiotu, urządzenia lub substancji, które mogą zagrozić zdrowiu lub życiu pasażerów lub załogi lub zniszczyć statek powietrzny albo spowodować jego uszkodzenia, mogące uniemożliwić jego lot lub stanowić zagrożenie bezpieczeństwa tego statku w czasie lotu;
5. porwaniu statku powietrznego z załogą i pasażerami na pokładzie lub bez nich, również w celu użycia statku powietrznego jako narzędzia ataku terrorystycznego z powietrza;
6. zniszczeniu albo uszkodzeniu lotniczych urządzeń naziemnych lub pokładowych, zakłóceniu ich działania lub użyciu przemocy wobec osoby obsługującej te urządzenia, w przypadku gdy powoduje to znaczne zakłócenie ruchu lotniczego lub zagrożenie bezpieczeństwa lotnictwa cywilnego;
7. przekazaniu nieprawdziwej informacji, która powoduje zagrożenie osób i mienia w komunikacji lotniczej;
8. zniszczeniu albo poważnym uszkodzeniu urządzeń na lotnisku, zakłóceniu ich działania lub użyciu przemocy wobec osoby obsługującej te urządzenia, w przypadku gdy powoduje to znaczne zakłócenie ruchu lotniczego lub funkcjonowania lotniska lub zagrożenie bezpieczeństwa lotnictwa cywilnego;
9. audyt ochrony - oznacza szczegółową analizę środków i procedur ochrony, mającą na celu stwierdzenie, czy są one w pełni stosowane w sposób ciągły;
10. audytor krajowy - rozumie się przez to audytora krajowego kontroli jakości w zakresie ochrony lotnictwa cywilnego;
11. audytor wewnętrzny - rozumie się przez to audytora wewnętrznego kontroli jakości w zakresie ochrony lotnictwa cywilnego;
12. czynności audytorskie - to czynności kontroli jakości w zakresie ochrony lotnictwa cywilnego, o których mowa w załączniku II do rozporządzenia 300/2008 oraz KPKJ;
13. inspekcja - oznacza analizę wdrożenia środków i procedur ochrony w celu ustalenia, czy są one realizowane skutecznie i zgodnie z wymaganymi standardami, a także w celu stwierdzenia ewentualnych uchybień;
14. kontrola dostępu - oznacza stosowanie środków, dzięki którym można zapobiec przedostaniu się nieupoważnionych osób lub nieupoważnionych pojazdów, lub zarówno nieupoważnionych osób, jak i nieupoważnionych pojazdów;
15. środki kontroli w zakresie ochrony - oznacza stosowanie środków, dzięki którym można zapobiec wprowadzeniu przedmiotów zabronionych;
16. KPKJ – rozumie się przez to Krajowy Program Kontroli Jakości w zakresie ochrony lotnictwa cywilnego ustalony w przepisach wydanych na podstawie art. 189 ust. 2 ustawy;
17. KPOLC – rozumie się przez to Krajowy Program Ochrony Lotnictwa Cywilnego ustalony w przepisach wydanych na podstawie art. 187 ustawy;
18. KPS – rozumie się przez to Krajowy Program Szkolenia w zakresie ochrony lotnictwa cywilnego ustalony w przepisach wydanych na podstawie art. 189 ust. 3 ustawy;
19. ładunek - oznacza każde mienie przeznaczone do przewożenia statkiem powietrznym, inne niż bagaż, poczta, poczta przewoźnika lotniczego, materiały przewoźnika lotniczego oraz zaopatrzenie pokładowe;
20. ochrona lotnictwa - oznacza połączenie środków oraz zasobów ludzkich i materialnych przeznaczonych do ochrony lotnictwa cywilnego przed aktami bezprawnej ingerencji, które zagrażają bezpieczeństwu lotnictwa cywilnego;
21. państwo pobytu - oznacza każdy kraj, w którym osoba przebywała stale przez 6 miesięcy lub dłużej, a „przerwa” w udokumentowanym kształceniu lub zatrudnieniu oznacza przerwę przekraczającą 28 dni;
22. sprawdzenie przeszłości - oznacza sprawdzenie, o którym mowa w pkt 11.1.3 załącznika do rozporządzenia 1998/2015;
23. sytuacja kryzysowa w lotnictwie cywilnym **-** oznacza zagrożenie wystąpieniem lub możliwością wystąpienia aktu bezprawnej ingerencji w lotnictwie cywilnym;
24. uchybienie - oznacza niespełnienie wymogu w zakresie ochrony lotnictwa;
25. ustawa - to ustawa z dnia 3 lipca 2002 roku – Prawo lotnicze;
26. wewnętrzna kontrola zgodności - oznacza czynności kontroli jakości w zakresie ochrony lotnictwa cywilnego realizowane na poziomie podmiotu prowadzącego działalność lotniczą, obejmującą audyty ochrony, wewnętrzne testy ochrony, inspekcje ochrony;
27. wewnętrzny test ochrony - oznacza sprawdzenie skuteczności stosowania środków ochrony przez podmioty prowadzące działalność lotniczą;
28. wywiad - oznacza ustną kontrolę przeprowadzoną przez audytora w celu ustalenia, czy wdrożono szczegółowe środki lub procedury ochrony;
29. zarejestrowany agent - oznacza przewoźnika lotniczego, agenta, spedytora lub inny podmiot zapewniający stosowanie środków kontroli w zakresie ochrony w odniesieniu do ładunku lub poczty;
30. znany nadawca - oznacza nadawcę, który wysyła ładunek lub pocztę na swój rachunek i którego procedury są zgodne ze wspólnymi zasadami i normami ochrony w stopniu wystarczającym, aby zezwolić na przewóz ładunku lub poczty każdym statkiem powietrznym.

**Definicje własne:**

*Jeżeli będzie to uzasadnione, proszę o stworzenie listy własnych definicji pojęć używanych w programie ochrony.*

##  Uregulowania prawne.

### Międzynarodowe uregulowania prawne.

1. Konwencja o międzynarodowym lotnictwie cywilnym, podpisana w Chicago dnia 7 grudnia 1944 r. - Konwencja chicagowska (Dz. U z 1959 r. Nr 35, poz. 212, z późn. zm.);
2. Konwencja w sprawie przestępstw i niektórych innych czynów popełnionych na pokładzie statków powietrznych, sporządzona w Tokio 14 września 1963 r. (Dz. U. z 1971 r. Nr 15, poz. 147);
3. Konwencja o zwalczaniu bezprawnego zawładnięcia statkami powietrznymi, sporządzona w Hadze 16 grudnia 1970 r.  (Dz. U z 1972 r. Nr 25, poz. 181);
4. Konwencja o zwalczaniu bezprawnych czynów skierowanych przeciwko bezpieczeństwu lotnictwa cywilnego, sporządzona w Montrealu dnia 23 września 1971 r. (Dz. U z 1976 r. Nr 8, poz. 37);
5. Konwencja w sprawie znakowania plastycznych materiałów wybuchowych w celu ich wykrycia, sporządzona w Montrealu dnia 1 marca 1991 r. (Dz. U. 2007 Nr 135, poz. 948);

### Unijne uregulowania prawne

1. Rozporządzenie Parlamentu Europejskiego i Rady (WE) Nr 300/2008 z dnia 11 marca 2008 r. w sprawie wspólnych zasad w dziedzinie ochrony lotnictwa cywilnego i uchylające rozporządzenie (WE) Nr 2320/2002 (Dz. Urz. UE L 97 z 9.4.2008);
2. Rozporządzenie Komisji (WE) Nr 272/2009 z dnia 2 kwietnia 2009 r. uzupełniającego wspólne podstawowe normy ochrony lotnictwa cywilnego określone w załączniku do rozporządzenia (WE) 300/2008 Parlamentu Europejskiego i Rady (Dz. Urz. UE L 91 z 3.4.2009 z późn. zmianami)
3. Rozporządzenie Komisji (UE) Nr 1254/2009 z dnia 18 grudnia 2009 r. ustanawiające kryteria pozwalające państwom członkowskim na odstępstwo od wspólnych podstawowych norm ochrony lotnictwa cywilnego i przyjęcie alternatywnych środków w zakresie ochrony (Dz. Urz. UE L 338 z 19.12.2009)
4. Rozporządzenie Wykonawcze Komisji (UE) Nr 2015/1998 z dnia 5 listopada 2015 r. ustanawiające szczegółowe środki w celu wprowadzenia w życie wspólnych podstawowych norm ochrony lotnictwa cywilnego (Dz. Urz. UE L 299 z 14.11.2015)
5. Decyzja wykonawcza Komisji C(2015) 8005 ustanawiająca szczegółowe środki w celu wprowadzenia w życie wspólnych podstawowych norm ochrony lotnictwa cywilnego obejmujących informacje, o których mowa w art. 18 lit. a) rozporządzenia (WE) nr 300/2008 z późn. zmianami.

### Krajowe uregulowania prawne

1. Ustawa z dnia 3 lipca 2002 r. - Prawo lotnicze (Dz. U. z 2020 r. poz. 1970 z późń. zm.);
2. Rozporządzenie Ministra Infrastruktury z dnia 2 grudnia 2020 r. w sprawie Krajowego Programu Ochrony Lotnictwa Cywilnego (Dz.U. z 2021 r. poz. 17), zwane dalej „Krajowym Programem Ochrony Lotnictwa Cywilnego”;
3. Rozporządzenie Ministra Transportu, Budownictwa i Gospodarki Morskiej z dnia 15 marca 2013 r. w sprawie szczegółowych wymagań dotyczących programów ochrony w lotnictwie cywilnym, (Dz. U. z 2021 r. poz. 407);
4. Rozporządzenie Ministra Transportu, Budownictwa i Gospodarki Morskiej z dnia 20 września 2013 r. w sprawie Krajowego Programu Szkolenia w zakresie ochrony lotnictwa cywilnego (Dz. U. z 2016 r. poz. 1852);
5. Rozporządzenie Ministra Infrastruktury z dnia 5 listopada 2020 r. w sprawie Krajowego Programu Kontroli Jakości w zakresie ochrony lotnictwa cywilnego (Dz. U. z 2020 r. poz. 2037).

## Struktura organizacyjna

##  Zakres i charakter prowadzonej działalności.

*Krótki opis przedmiotu działalności przedsiębiorcy. Wyszczególnienie, jakie produkty będą wysyłane transportem lotniczym w ramach statusu znanego nadawcy.*

##  Struktura organizacyjna przedsiębiorstwa

*Schemat organizacji przedsiębiorstwa, z uwzględnieniem usytuowania w nim osoby odpowiedzialnej za ochronę i audytora wewnętrznego.*

## Osoba odpowiedzialna ochronę.

Za ochronę przedsiębiorstwa w zakresie ochrony lotnictwa cywilnego odpowiedzialny jest Kierownik ds. Ochrony Znanego Nadawcy (Security Manager). Kierownik ds. Ochrony Znanego Nadawcy może powierzyć część swoich uprawnień wyznaczonemu pracownikowi zajmującemu odpowiednie do zakresu uprawnień stanowisko, pełnomocnictwa i posiadającemu odpowiednie kwalifikacje.

Kierownik ds. Ochrony: …………………………………..

Stanowisko służbowe: ……………………………………

Tel. stacjonarny/komórkowy: ……………………………..

Adres e-mail: …………………………………..................

Zastępca Kierownika ds. Ochrony: ………………………

Stanowisko służbowe: ……………………………………

Tel. stacjonarny/komórkowy: ……………………………..

Adres e-mail: …………………………………...............

Kierownik ds. Ochrony Znanego Nadawcy jest zobowiązany w szczególności do:

1. opracowania, realizacji i aktualizacji Programu Ochrony Znanego Nadawcy;
2. zapewnienia wdrożenia postanowień Programu Ochrony i jego procedur;
3. zapewnienia realizacji wewnętrznej kontroli zgodności;
4. utrzymywania kontaktów w zakresie ochrony i bezpieczeństwa przewozów z Departamentem Ochrony w Lotnictwie Cywilnym Urzędu Lotnictwa Cywilnego;
5. sprawowania nadzoru nad firmami działającymi na rzecz Znanego Nadawcy na zlecenie oraz odpowiedzialnymi za ochronę obiektów podmiotu w ramach obowiązujących procedur;
6. znajomości krajowych oraz unijnych uregulowań prawnych oraz procedur ochrony przed aktami bezprawnej ingerencji;
7. wnioskowania i wdrażania nowych rozwiązań w obszarze ochrony lotnictwa cywilnego w Przedsiębiorstwie;
8. informowania Prezesa Urzędu Lotnictwa Cywilnego oraz Szefa Agencji Bezpieczeństwa Wewnętrznego informacji o zagrożeniu aktami bezprawnej ingerencji w zakresie obsługi identyfikowalnych ładunków lotniczych oraz o wszelkich zagrożeniach, co do których istnieją przesłanki, że mogą one skutkować aktami bezprawnej ingerencji w lotnictwie cywilnym;
9. zapewnienie przedstawicielom Urzędu warunków do wykonywania na terenie podmiotu obowiązków służbowych w zakresie ochrony lotnictwa cywilnego;

## Środki ochrony

##  Ochrona fizyczna

|  |
| --- |
| 1. Opis obiektów znajdujących się na terenie lokalizacji Znanego Nadawcy |
| Krótki opis lokalizacji z uwzględnieniem konstrukcji budynków (np. obiekt kontenerowy, budynek murowany), ich przeznaczenie (np. produkcja, magazynowanie, handel) oraz opis powierzchni. |
| 2. Opis ogrodzenia |
| Czy obiekt jest/nie jest ogrodzony.Charakterystyka ogrodzenia (wysokość, długość, rodzaj zastosowanego materiału) oraz sposób zabezpieczenia (np.: concertina, systemy elektroniczne). Czy ogrodzenie jest monitorowane. Czy przy ogrodzeniu znajdują się przedmioty ułatwiające przedostanie się przez ogrodzenie.Liczba oraz lokalizacja punktów dostępu do obiektu przez ogrodzenie dla osób/pojazdów. |
| 3. Kontrola dostępu osób |
| Czy została wprowadzona kontrola dostępu osób na teren obiektu.Sposób realizacji kontroli dostępu na teren obiektu (środki osobowe, system elektroniczny, inne).Rodzaj dokumentu wewnętrznego upoważniającego do dostępu na teren obiektu/do wydzielonych stref. Procedury nadawania uprawnień dostępu na teren obiektu/do wydzielonych stref.Osoba/komórka odpowiedzialna za wydawanie upoważnień na teren obiektu/do wydzielonych stref.Procedury dostępu dla gości na teren obiektu/do wydzielonych stref.Lokalizacja urządzeń (np. serwer, kontroler, router), wykorzystywanych przez elektroniczny system kontroli dostępu oraz osoby mające do nich dostęp. |
| 4. Kontrola dostępu pojazdów |
| Czy została wprowadzona kontrola dostępu pojazdów na teren obiektu/do strefy wysyłki.Sposób realizacji kontroli dostępu pojazdów na teren obiektu/do strefy wysyłki (środki osobowe, system elektroniczny, inne).Rodzaj dokumentu wewnętrznego upoważniającego do dostępu pojazdów na teren obiektu/do strefy wysyłki. Procedury nadawania uprawnień dostępu pojazdom na teren obiektu/do strefy wysyłki.Osoba/komórka odpowiedzialna za wydawanie upoważnień dostępu pojazdom na teren obiektu/do strefy wysyłki.Procedury dostępu pojazdów na teren obiektu/do strefy wysyłki osób nie będących pracownikami podmiotu.Lokalizacja urządzeń (np. serwer, kontroler, router), wykorzystywanych przez system kontroli dostępu oraz osoby mające do nich dostęp. |
| 5. Techniczne środki ochrony |
| Czy zainstalowano system CCTV.Obszary objęte nadzorem CCTV. Czy obrazy CCTV są stale rejestrowane. Sposób rejestracji obrazów. Czas przechowywania zapisów.Administrator systemu CCTV. Osoba odpowiedzialna za weryfikację poprawności funkcjonowania systemu CCTV.Czy są stosowane systemy sygnalizacji włamania i napadu, detekcji ruchu. Kto nimi administruje.Lokalizacja serwerów dla systemu CCTV i pozostałych systemów ochrony oraz sposoby ich ochrony przed dostępem osób nieupoważnionych. |
| 6. Środki osobowe |
| Liczba i obsada posterunków ochrony.Czy obiekt jest patrolowany. Obszary objęte patrolowaniem i częstotliwość patroli.Kto odpowiada za obsadę posterunków i realizację patroli. W przypadku korzystania z usługodawców zewnętrznych proszę o podanie podstaw współpracy (np.: umowa, porozumienie). |
| 7. Dodatkowe informacje |
| Inne informacje dotyczące stosowanych środków ochrony fizycznej. |

## Produkcja

|  |
| --- |
| Opis stref wydzielonych do ochrony identyfikowalnych ładunków lotniczych w miejscu produkcji.Sposób zabezpieczenia miejsca produkcji identyfikowalnych ładunków lotniczych (kontrola dostępu, systemy alarmowe, CCTV). Jeżeli przedmiotowe procedury zostały opisane we wcześniejszych punktach dokumentu, należy odwołać się do odpowiedniego opisu/punktu.Środki kontroli zapobiegające naruszeniu IPL na etapie produkcji. |

## Pakowanie

|  |
| --- |
| Opis stref wydzielonych do ochrony identyfikowalnych ładunków lotniczych w miejscu przeznaczonym na pakowanie identyfikowalnych ładunków lotniczych.Czy proces pakowania jest nadzorowany? Sposób zabezpieczenia miejsca pakowania (kontrola dostępu, systemy alarmowe, CCTV). Jeżeli przedmiotowe procedury zostały opisane we wcześniejszych punktach dokumentu, należy odwołać się do odpowiedniego opisu/punktu.Opis opakowania zewnętrznego, jednostkowego lub zbiorczego – w zależności od wdrożonych procedur. Materiał, z którego wykonano opakowanie. Jego wytrzymałość. Systemu używane do otwierania/zamykania/zabezpieczania opakowań jednostkowych/opakowań zbiorczych (taśmy spinające, taśmy pakowe, kołki rozporowe, zatrzaski, zamki etc.).Czy gotowe opakowanie zewnętrzne jest zabezpieczone w sposób umożliwiający łatwe stwierdzenie jego naruszenia? Opis sposobu zabezpieczenia opakowań jednostkowych lub zbiorczych (np.: stosowane plomby, taśmy zabezpieczające, pieczęcie, etc.). Wskazane jest dodanie dokumentacji fotograficznej stosowanego zabezpieczenia opakowania. Wzory stosowanych plomb lub innych zabezpieczeń.Czy plomby, taśmę zabezpieczającą lub specjalne pieczęcie przechowuje się w bezpiecznych warunkach, gdy nie są używane? Kto ma do nich dostęp? W jaki sposób są one rozliczane?Opis procedury ewidencjonowania i rozliczania stosowanych plomb lub/i jeżeli dotyczy innych zabezpieczeń, rejestrów oraz podanie ich wzorów.Osoba odpowiedzialna za rozliczanie plomb lub/i jeżeli dotyczy innych zabezpieczeń. |

##  Składowanie

|  |
| --- |
| Opis stref wydzielonych do ochrony identyfikowalnych ładunków lotniczych w miejscu przeznaczonym na składowanie identyfikowalnych ładunków lotniczych.Opis miejsca składowania ładunków przeznaczonych do transportu lotniczego.Sposób zabezpieczenia miejsca składowania (kontrola dostępu, systemy alarmowe, CCTV). Jeżeli przedmiotowe procedury zostały opisane we wcześniejszych punktach dokumentu, należy odwołać się do odpowiedniego opisu/punktu.Wskazanie osób z dostępem do miejsca składowania (proszę o podanie stanowisk). |

* 1. **Wysyłka**

|  |
| --- |
| Opis stref wydzielonych do ochrony identyfikowalnych ładunków lotniczych w miejscu przeznaczonym na wysyłkę identyfikowalnych ładunków lotniczych.Opis procedury wysyłki, od momentu złożenia zamówienia na towar, poprzez wybór konkretnego egzemplarza, wybór środka transportu, przygotowanie dokumentacji transportowej, przekazanie przesyłki lotniczej przewoźnikowi drogowemu.Osoby mające dostęp do systemów komputerowych wykorzystywanych podczas procedury wysyłki oraz zabezpieczenie tych systemów. Czy została wyznaczona strefa wysyłki odrębna od strefy składowania, gdzie identyfikowalne przesyłki lotnicze oczekują na transport. Zasady kontroli dostępu do strefy wysyłki i nadzór nad strefą. |

## Przesyłka z innych źródeł

|  |
| --- |
| Czy przedsiębiorstwo przyjmuje, zawierające ładunek, przesyłki przeznaczone do przewozu lotniczego od innych przedsiębiorstw?Jeśli tak, w jaki sposób przesyłki te są oddzielane od własnego ładunku przedsiębiorstwa i w jaki sposób są wskazywane zarejestrowanemu agentowi/przewoźnikowi? |

* 1. **Przewóz**

|  |
| --- |
| Opis, w jaki sposób ładunek lotniczy opuszcza teren lokalizacji i jest przekazywany zarejestrowanemu agentowi:* jest odbierany przez zarejestrowanego agenta bądź w jego imieniu,
* własnymi środkami transportu znanego nadawcy,
* przez podwykonawcę, z którego usług korzysta znany nadawca.

Procedura awizowania transportu drogowego, weryfikacji kierowcy i załadunku.Opis stosowanych środków transportu (np. pojazdy z zamkniętym przedziałem ładunkowym, otwarte platformy etc.).Informacja o wymogu podpisania deklaracji przewoźnika drogowego przez podwykonawcę.Sposób zabezpieczenia przestrzeni ładunkowej pojazdu. Kto odpowiada za zabezpieczenie przestrzeni ładunkowej pojazdu (znany nadawca czy zarejestrowany agent).Kto zabezpiecza przestrzeń ładunkową pojazdu (kierowca czy pracownik zakładu).Wzory stosowanych plomb lub innych zabezpieczeń. Czy plomby i inne zabezpieczenia przechowuje się w bezpiecznych warunkach, gdy nie są używane? Opis procedury ewidencjonowania i rozliczania stosowanych plomb lub/i jeżeli dotyczy innych zabezpieczeń, rejestrów oraz podanie ich wzorów.Osoba odpowiedzialna za rozliczanie plomb lub/i jeżeli dotyczy innych zabezpieczeń. |

## 3.8 Cyberbezpieczeństwo

|  |
| --- |
| W ramach realizacji przepisów, o ile podmiot nie jest operatorem usług kluczowych, proszę o identyfikację krytycznych systemów technologii informacyjno-komunikacyjnych jako systemów informacyjnych w rozumieniu ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa, przeznaczonych do przetwarzania danych wykorzystywanych dla bezpieczeństwa, ochrony lub dostępności operacji lotniczych.W tym kontekście proszę o opisanie systemów lub o informację, że takowych Państwo nie posiadają (wówczas pozostałe kwestie nie muszą być poruszone);Opisanie sposobu prowadzenia oceny ryzyka oraz wdrażania środków mających na celu ochronę krytycznych systemów i danych przed bezprawną ingerencją. W tym kontekście proszę o opisanie odpowiedzialności w tym zakresie.Szczegółowe określenie środków mających na celu zapewnienie ochrony przed cyberatakami, które mogłyby wpłynąć na bezpieczeństwo lotnictwa cywilnego, wykrywania ich i reagowania na nie. Opisanie środków i miejsca zgłaszania incydentu (ścieżka zgłaszania na zewnątrz organizacji).Informacja o zapewnieniu, że osoby wdrażające ww. środki posiadają kwalifikacje i umiejętności niezbędne do skutecznego wykonywania wyznaczonych zadań oraz są one informowane o istotnych przypadkach zagrożeń dla cyberbezpieczeństwa, zgodnie z zasadą ograniczonego dostępu. Odniesienie się czy zapewniają Państwo odpowiednie szkolenia dla osób wdrażających środki z zakresu cyberbezpieczeństwa, ewentualnie, że weryfikują Państwo (jeżeli ma to zastosowanie), kwalifikacje i umiejętności takich osób przy naborze lub przed zawarciem umowy cywilno-prawnej. Opisanie procedur informowania o incydentach wewnątrz organizacji. |

## Wewnętrzna kontrola jakości w zakresie ochrony lotnictwa cywilnego

##  Formy prowadzenia wewnętrznej kontroli zgodności

*Nazwa przedsiębiorcy* stosuje następujące rodzaje wewnętrznej kontroli zgodności realizowane przez audytorów wewnętrznych zgodnie z Krajowym Programem Kontroli Jakości:

1) audyt ochrony;

2) inspekcję ochrony;

3) wewnętrzny test ochrony.

W celu potwierdzenia stosowania środków ochrony, przeprowadzenie audytu ochrony opiera się na systematycznym gromadzeniu informacji z zastosowaniem jednej lub kilku z poniższych technik:

a) analiza dokumentów;

b) obserwacje;

c) wywiady;

d) weryfikacje.

##  Harmonogram wewnętrznej kontroli zgodności.

Częstotliwość przeprowadzania wewnętrznej kontroli zgodności przez Znanego Nadawcę oparta jest na sporządzeniu rocznego harmonogramu wewnętrznej kontroli zgodności w terminie do końca grudnia każdego roku kalendarzowego na rok następny.

Roczny harmonogram wewnętrznej kontroli zgodności jest tworzony na podstawie analizy ryzyka wykonywanej przez Znanego Nadawcę z uwzględnieniem kryteriów:

* wyników kontroli zgodności w zakresie ochrony lotnictwa cywilnego,
* wyników kontroli w zakresie ochrony lotnictwa cywilnego, przeprowadzonych przez audytorów Unii Europejskiej, Organizacji Międzynarodowego Lotnictwa Cywilnego oraz Europejskiej Konferencji Lotnictwa Cywilnego,
* konsekwencji zaistniałych uchybień w systemie ochrony podmiotu kontrolowanego,
* ilości odprawionych ładunków,
* liczby incydentów lotniczych mających wpływ na poziom ochrony lotnictwa cywilnego oraz rodzaju i skali prowadzonej działalności lotniczej oraz liczby lokalizacji, w których jest prowadzona działalność lotnicza.

Wewnętrzna kontrola zgodności obejmuje w roku kalendarzowym weryfikację, poprzez inspekcje lub audyty ochrony, elementów tj.:

1. wszystkich przepisów dotyczących kontroli środków ochrony stosowanych przez znanych nadawców oraz
2. wszystkie przepisy dotyczące przewozu ładunków i poczty;

Każdy ze środków ochrony, o którym mowa powyżej w punktach a) oraz b) podlega testowi ochrony przynajmniej raz na kwartał.

Testy przeprowadza się, aby sprawdzić skuteczność zabezpieczenia IPL przed nieuprawnionym dostępem.

## Dokumentacja wewnętrznej kontroli zgodności i sprawozdawczość.

Znany Nadawca prowadzi wewnętrzną kontrolę zgodności w sposób ciągły oraz udokumentowany.

Dokumentacja przechowywana jest przez okres co najmniej trzech lat i zawiera informacje o zakresie, wynikach wewnętrznej kontroli zgodności oraz imionach i nazwiskach osób biorących w niej udział.

Z przeprowadzonych czynności audytorskich audytor wewnętrzny sporządza wewnętrzny raport końcowy uwzględniający następujące elementy:

1) Dane dotyczące:

* terminu przeprowadzenia czynności audytorskich,
* składu zespołu audytorskiego,
* podmiotu kontrolowanego, uwzględniające wszystkich jego przedstawicieli uczestniczących w czynnościach audytorskich,

2) Zestawienie sprawdzonych elementów systemu ochrony, ze szczegółowym opisem stwierdzonych uchybień odnośnie stanu faktycznego w świetle obowiązujących przepisów z zakresu ochrony lotnictwa cywilnego oraz przyznane kategorie systemu klasyfikacji zgodności,

3) Zalecenia i wnioski pokontrolne, odnoszące się do każdego sprawdzonego elementu systemu ochrony, wraz z opisem działań korygujących, które obowiązany jest podjąć podmiot kontrolowany,

4) Działania korygujące wobec stwierdzonych uchybień.

Przygotowany wewnętrzny raport końcowy przekazywany jest do Kierownika ds. Ochrony.

Kierownik ds. Ochrony ma obowiązek przygotowania programu naprawczego w terminie do 10 dni po otrzymaniu wewnętrznego raportu końcowego z przeprowadzonych czynności audytorskich w odniesieniu do stwierdzonych niezgodności, o których mowa powyżej. Program naprawczy uwzględnia następujące elementy:

* termin usunięcia uchybienia,
* sposób realizacji działań naprawczych w stosunku do stwierdzonych uchybień,
* osobę odpowiedzialną za realizację działań naprawczych.

Z chwilą zakończenia działań korygujących w ramach programu naprawczego, audytor wewnętrzny ustala termin czynności audytorskich sprawdzających wdrożenie przedsięwzięć naprawczych określonych w ww. programie naprawczym.

Znany Nadawca przesyła Prezesowi Urzędu Lotnictwa Cywilnego roczne sprawozdanie z przeprowadzonej wewnętrznej kontroli zgodności w terminie do końca stycznia każdego roku kalendarzowego za rok poprzedni.

## Wymagania dotyczące personelu.

##  Sprawdzenie przeszłości

Zgodnie z postanowieniami rozporządzenia 1998/2015 oraz § 32 KPOLC, Kierownik ds. Ochrony, oraz wszystkie osoby obsługujące przesyłki lotnicze przechodzą sprawdzenie przeszłości obejmujące:

* ustalenie tożsamości osoby na podstawie dokumentu potwierdzającego tożsamość;
* informacje z rejestrów karnych ze wszystkich państw pobytu, w rozumieniu pkt 11.0.3 załącznika do rozporządzenia 1998/2015, z co najmniej 5 poprzedzających lat albo uzyskanie informacji o braku negatywnych przesłanek na podstawie art. 188a ust. 4 ustawy Prawo lotnicze z dnia 3 lipca 2002 r. z późn. zm.;
* informacje o zatrudnieniu i kształceniu oraz o wszystkich okresach przerw w zatrudnieniu i kształceniu, z co najmniej 5 poprzedzających lat.

Sprawdzanie przeszłości pracowników na stanowiskach związanych z obsługą przesyłek lotniczych i poczty lotniczej odbywa się nie rzadziej niż raz na 5 lat.

Kierownik ds. ochrony wyjaśnia powody każdej przerwy w zatrudnieniu lub kształceniu osoby poddawanej sprawdzeniu przeszłości przekraczające 28 dni.

Dokumentacja dotycząca sprawdzenia przeszłości przechowywana jest w ……. Za nadzór nad dokumentacją odpowiedzialny jest …….

## Szkolenia

Nadzór nad szkoleniami w zakresie ochrony lotnictwa pełni Kierownik ds. Ochrony Znanego Nadawcy.

Pracownicy podlegają następującym szkoleniom:

1. Szkolenie osób stosujących środki kontroli w zakresie ochrony ładunku i poczty inne niż kontrola bezpieczeństwa lub mających dostęp do identyfikowalnego ładunku lotniczego, albo identyfikowalnej poczty lotniczej ma na celu zdobycie następujących kwalifikacji (patrz pkt 11.2.3.9 – Rozporządzenie Wykonawcze Komisji (UE) Nr 2015/1998 z dnia 5 listopada 2015 r.) *– jakie grupy pracowników podlegają*
2. Szkolenie podstawowe osób wykonujących zadania wymienione w pkt. 11.2.4, 11.2.5 i 11.5 (patrz pkt. 11.2.2 – Rozporządzenie Wykonawcze Komisji (UE) Nr 2015/1998 z dnia 5 listopada 2015 r.). *– jakie grupy pracowników podlegają*
3. Specjalistyczne szkolenie osób bezpośrednio nadzorujących osoby stosujące środki kontroli w zakresie ochrony – przełożonych (patrz pkt. 11.2.4 – Rozporządzenie Wykonawcze Komisji (UE) Nr 2015/1998 z dnia 5 listopada 2015 r.) *– jakie grupy pracowników podlegają*
4. Specjalistyczne szkolenie osób ponoszących na szczeblu krajowym lub lokalnym ogólną odpowiedzialność za zapewnienie, by procedury ochrony i jego wdrożenie były zgodne ze wszystkimi przepisami prawa – tzw. Kierowników ds. ochrony (patrz pkt 11.2.5 – Rozporządzenie Wykonawcze Komisji (UE) Nr 2015/1998 z dnia 5 listopada 2015 r.). *– jakie grupy pracowników podlegają*
5. Szkolenie osób wymagających ogólnej świadomości w zakresie ochrony lotnictwa cywilnego – (patrz pkt. 11.2.7 – Rozporządzenie Wykonawcze Komisji (UE) Nr 2015/1998 z dnia 5 listopada 2015 r.) *– jakie grupy pracowników podlegają*

## Kultura ochrony oraz przeciwdziałanie zagrożeniom wewnętrznym.

1. Definicja, cele i polityka kultury ochrony.

Kultura ochrony to zbiór norm, przekonań, wartości, postaw i założeń związane z codziennym funkcjonowaniem, promowanych przez organizację w celu zapewnienia optymalnego poziomu ochrony. Wdrożenie skutecznej kultury ochrony zapewnia:

* + - uznanie, że skuteczna ochrona jest nie tylko wymogiem prawnym, ale także kluczowym warunkiem funkcjonowania organizacji;
		- promocję pozytywnych praktyk w zakresie ochrony wśród pracowników i podwykonawców;
		- powiązanie ochrony z podstawowymi celami organizacji;
		- traktowanie ochrony jako wartości podstawowej, nie uciążliwego obowiązku.
		- wprowadzenie w obszarze ochrony zasad Just Culture (kultury sprawiedliwego traktowania).

*Nazwa podmiotu* tworzy politykę kultury ochrony spełniającą następujące kryteria:

* Polityka jest akceptowana przez najwyższe władze (np. zarząd) podmiotu;
* Polityka dotyczy całego personelu podmiotu, łącznie z kierownictwem, oraz jego stałych podwykonawców;
* Polityka określa podstawowe zasady kultury ochrony, środki jej wdrażania i odpowiedzialność w tym zakresie.
1. Zagrożenia wewnętrzne.

2.1. Rodzaje zagrożeń

Zagrożenia wewnętrzne są to zagrożenia dla ochrony podmiotu wynikające z celowych działań szeroko rozumianego personelu. Zagrożenia wewnętrzne mogą wiązać się z:

* zachowaniami o charakterze kryminalnym,
* radykalizacją polityczną, religijną, ideologiczną lub inną, prowadzą do ekstremizmu i wykorzystującą/dopuszczającą akt terroru jako formę przekazywania/narzucania swoich przekonań i poglądów;
* terroryzmem.

Przez radykalizację należy rozumieć proces, w którym osoba lub grupa przybiera coraz bardziej skrajne poglądy, prowadzące do ekstremizmu. Ekstremizm polega na hołdowaniu skrajnym poglądom i w najbardziej radykalnych przypadkach dopuszcza użycie przemocy oraz wykorzystanie innych bezprawnych środków (tzw. brutalny ekstremizm). Radykalizująca się osoba może przyjmować coraz bardziej skrajne poglądy, a w dalszej kolejności uznać, że jedynym sposobem realizacji jej zamiarów jest terroryzm.

Prawo do wyrażania swoich opinii to jeden z podstawowych elementów demokracji. Wyraża się w formie **aktywizmu, który nie jest jednym z etapów radykalizacji i nie należy go mylić z ekstremizmem**.

Od przejawów radykalizacji lub ekstremizmu należy odróżnić zachowania związane z zaangażowaniem politycznym, religijnym i wspólnotowym, które charakteryzują się pokojową formą i wykorzystaniem akceptowalnych środków wyrazu.

* 1. Identyfikacja zagrożeń

W celu identyfikacji wskaźników radykalizacji można posłużyć się poniższymi przykładami:

Niegroźne zachowania:

Jeżeli dana osoba zachowuje się w opisany poniżej sposób, nie powinno budzić to obaw:

* + - Kłóci się z bliskimi osobami aby bronić swoich racji i przekonań.
		- Przyjmuje widoczne znaki (tradycyjne ubrania, długa broda, ogolona głowa, symbole religijne, określone tatuaże itp.), aby wyrazić swoją tożsamość lub poczucie przynależności do wybranej grupy;
		- Jest aktywna w mediach społecznościowych;
		- Zajmuje wyraźnie określone stanowisko i dyskutuje o sprawach związanych ze społecznością, daną grupą lub indywidualnymi osobami;
		- Wyraża żywe zainteresowanie bieżącymi sprawami krajowymi i międzynarodowymi;
		- Zwiększa swoje zaangażowanie w praktyki religijne lub w aktywność polityczną;
		- Zmienia wyznanie lub nabiera nowych przekonań ideologicznych lub politycznych;
		- Nalega na przestrzeganie określonej diety i innych zakazów wynikających z przekonań religijnych lub politycznych;
		- Wyraża potrzebę doznania nowych wrażeń i przygód;
		- Wyraża potrzebę walczenia z niesprawiedliwością.

Problematyczne zachowania:

Ta kategoria obejmuje zachowania, które świadczą o złym samopoczuciu danej osoby. Jeżeli zachowuje się ona w opisany poniżej sposób, to oznacza, że coraz mocniej utożsamia się z wybraną sprawą lub ideologią, co prowadzi do istotnych zmian w jej stylu życia:

* + - Wyraża spolaryzowane poglądy, których nie chce poddać pod dyskusję;
		- Jej zachowanie zaczyna powodować konflikty w życiu rodzinnym;
		- Fascynuje się teoriami spiskowymi i opowiada o nich;
		- Zaczyna izolować się od rodziny i (lub) znajomych;
		- Nagle zmienia swoje nawyki;
		- Ma poczucie odrzucenia i bycia ofiarą;
		- Uporczywie głosi swoje religijne lub polityczne przekonania;
		- Odrzuca zasady obowiązujące w organizacji, z którą jest związana (praca, szkoła drużyna sportowa itp.);
		- Odmawia udziału w zajęciach grupowych lub rezygnuje z kontaktów z innymi osobami z powodu: poglądów, rasy, koloru skóry, wyznania lub płci;
		- Wyraża potrzebę dominacji lub kontroli nad innymi osobami;
		- Nie chce zmienić swoich poglądów i uznać innych punktów widzenia.

Niepokojące zachowanie:

Kategoria obejmuje zachowania, które można wiązać z początkiem zaangażowania danej osoby w radykalną działalność. Charakteryzuje się dużą nieufnością do świata zewnętrznego oraz przewagą poglądów legitymizujących użycie przemocy do osiągnięcia własnych celów:

* + - Całkowicie zrywa więzi z rodziną lub znajomymi oraz utrzymuje relacje wyłącznie z nowo poznanymi osobami;
		- Usprawiedliwia użycie przemocy w celu obrony sprawy lub ideologii;
		- Ukrywa nowy styl życia lub system wartości przed członkami rodziny i bliskimi;
		- Nawiązuje relacje z osobami lub grupami o poglądach ekstremistycznych;
		- Nagle traci zainteresowanie pracą lub szkołą ;
		- Używa symboli i znaków związanych z ekstremistycznymi ugrupowaniami;
		- Wierzy w nagły koniec świata, męczeństwo lub inne mesjanistyczne wizje;
		- Wyraża nienawiść wobec innych osób lub grup.

Alarmujące zachowanie:

Ta kategoria obejmuje zachowania świadczące o niezwykle silnym przywiązaniu danej osoby do ideologii lub sprawy, które doprowadziło ją do przekonania, że przemoc jest jedynym możliwym i skutecznym środkiem działania:

* + - Bierze udział w działaniach grupy ekstremistycznej (materialnie, finansowo lub fizycznie);
		- Rekrutuje lub namawia osoby do przyłączenia się do grupy ekstremistycznej lub ekstremistycznego przedsięwzięcia;
		- Kontaktuje się z grupami lub osobami znanymi ze skrajnych poglądów (również przez internet);
		- Wzmacnia swoje przekonania przez odwiedzanie radykalnych stron i forów internetowych;
		- Planuje lub popełnia akty przemocy inspirowane radykalnymi poglądami;
		- Interesuje się bronią i (lub) materiałami wybuchowymi, materiałami niebezpiecznymi (tzw. DGR) bezprawnie stara się je nabyć lub uczy się nimi posługiwać;
		- Planuje podróż do strefy konfliktu lub regionu, w którym aktywne są grupy ekstremistyczne lub terrorystyczne.
	1. Zapobieganie

System zapobiegania zagrożeniom wewnętrznym obejmuje:

* okresowe sprawdzenia przeszłości personelu, zgodnie z rozdziałem …. Programu ochrony;
* działania podnoszące świadomość ochrony personelu;
* monitorowanie;
* system zgłaszania zdarzeń;
* inne działania *(skrótowo opisać jakie).*
1. System zgłaszania zdarzeń.

Wszelkie zdarzenia związane z ochroną, w tym zagrożeniami wewnętrznymi, mogą być zgłaszane w następujący sposób:

* bezpośrednio, ustnie, do:
	+ przełożonego;
	+ kierownika ds. ochrony;
* drogą elektroniczną (e-mail, korporacyjne platformy komunikacji wewnętrznej) na adres:
	+ ………………..;
	+ bezpośredniego przełożonego;
* telefonicznie, na numer:
	+ ……………………….;
	+ bezpośredniego przełożonego;
* dokumentem papierowym, złożonym w:
	+ ….….;
	+ ………

Dostęp do danych osobowych osób zgłaszających nieanonimowo mają wyłącznie osoby odbierające i analizujące zgłoszenie.

Nie podejmuje się działań w celu ustalenia tożsamości osób składających zgłoszenia anonimowe, z wyłączeniem sytuacji, w których zgłaszający przyznaje się do popełnienia przestępstwa.

Wszystkie zgłoszenia zdarzeń dot. zagrożeń wewnętrznych - niezależnie od ich wagi i charakteru – są przechowywane, ze względu na fakt, że ich znaczenie może się okazać istotne dopiero w późniejszym czasie.

Analizie podlegają wszystkie zgłoszenia, zarówno anonimowe jak i podpisane. Za analizę zgłoszeń odpowiada …. …..

Analiza jest prowadzona niezwłocznie po otrzymaniu zgłoszenia.

Wyniki analizy zgłoszenia:

1. Jeżeli informacja wskazuje na wiarygodne zagrożenie aktem bezprawnej ingerencji, podejmuje się działania zgodne z procedurami zawartymi w rozdziale ….. programu ochrony „Planowanie działań na wypadek sytuacji kryzysowych”.
2. Jeżeli informacja wskazuje na wiarygodną możliwość popełnienia przestępstwa, jest przekazywana do ………………………….., w celu podjęcia decyzji o ewentualnym złożeniu zawiadomienia o możliwości popełnienia przestępstwa do:
* właściwej miejscowo jednostki Policji lub prokuratury;
* właściwego miejscowo komendanta oddziału Straży Granicznej, w przypadku spraw dotyczących nielegalnej migracji, zapewnienie bezpieczeństwa w komunikacji międzynarodowej i porządku publicznego w zasięgu terytorialnym przejścia granicznego lub innych przestępstw zakresie właściwości Straży Granicznej.
1. Jeżeli informacja wskazuje na wysokie prawdopodobieństwo radykalizacji członka personelu, a w szczególności występują zachowania określone w punkcie „Identyfikacja zagrożeń” jako alarmujące, ……………………………….. podejmuje decyzję o przekazaniu informacji do właściwej miejscowo delegatury ABW, a w przypadku podmiotów prowadzących działalność lotniczą znajdujących się we właściwości terytorialnej Centrali ABW – również CAT ABW.
2. Jeżeli informacja wskazuje na niewystarczającą skuteczność stosowanych procedur ochrony, kierownik ds. ochrony przeprowadza analizę możliwości wprowadzenia stosownych zmian.

W przypadkach, w których dochodzi do oceny odpowiedzialności konkretnych osób, organizacja skupia się na ustaleniu, czy działania, zaniedbania bądź podjęte decyzje były adekwatne do doświadczenia i wyszkolenia, a nie do rezultatów zdarzenia.

Ponadto, co …… (*nie rzadziej niż corocznie*) dokonuje się analizy zbiorczej wszystkich otrzymanych zgłoszeń w celu ustalenia powtarzających się problemów i aktualnych tendencji oraz wypracowania zasad przeciwdziałania nim.

1. Wdrożenie, utrzymanie i rozwój kultury ochrony

|  |  |  |  |
| --- | --- | --- | --- |
| Lp. | *Rodzaj działania* | *Odniesienie do dokumentów wewnętrznych lub opis wdrożonych rozwiązań* | *Osoba odpowiedzialna* |
| 1. | Wdrożenie Systemu Zarządzania Ochroną (Security Management System – SeMS).*(optymalnym jest skrótowo wskazać czy w Podmiocie jest wdrożony SeMS a jeśli nie w jakim trybie zarządza się ochroną).* |  |  |
| 2. |

|  |
| --- |
| Tworzenie i aktualizacja dokumentów bezpośrednio odnoszących się do kultury ochrony i zagrożeń wewnętrznych ( np. polityka, procedury zgłaszania).*(optymalnym jest opisać jakie to dokumenty).* |
|  |

 |  |  |
| 3. | Włączanie odniesień do kultury ochrony w dokumentach firmowych (strategiach, planach, procedurach, opisach procesów itp.) nie związanych bezpośrednio z ochroną.*(optymalnym jest skrótowo opisać jakie to dokumenty).* |  |  |
| 4. | Planowanie stałych, okresowych i doraźnych działań informacyjnych promocyjnych dotyczących zagrożeń dla ochrony i promujących kulturę ochrony.*(optymalnym jest skrótowo opisać w jakich dokumentach zawarte są odniesienia do planowanych działań).* |  |  |
| 5. | Przygotowanie treści dotyczących kultury ochrony i zagrożeń wewnętrznych przekazywanych w ramach szkoleń z zakresu ochrony |  |  |
| 6. | Analiza zgłoszeń otrzymanych w ramach systemu zgłaszania.*(optymalnym jest skrótowo opisać w jaki sposób jest prowadzona analiza zgłoszeń – z podziałem na ocenę zagrożenia i analizę ryzyka).* |  |  |
| 7. | Kontrola jakości w zakresie elementów kultury ochrony.  |  |  |

## Zarządzanie kryzysowe

##  Procedury postępowania na wypadek nieuprawnionego dostępu do ładunków lotniczych lub poczty lotniczej.

W przypadku wykrycia wtargnięcia lub próby wtargnięcia osób nieuprawnionych na teren znanego nadawcy bądź groźby skierowanej przeciwko osobom, urządzeniom, środkom transportu znajdującym się w strefie przedsiębiorstwa należy niezwłocznie poinformować o tym fakcie:

*Imię nazwisko*

*Telefon*

*e-mail*

Wszyscy pracownicy powinni zwracać uwagę na osoby, które nie posiadają odpowiednich ważnych przepustek osobowych/samochodowych, a przebywają w pobliżu strefy zastrzeżonej – skontrolowanego, identyfikowalnego ładunku/towaru albo wykazują nim nieuzasadnione zainteresowanie i niezwłocznie informować osoby odpowiedzialne za ochronę,

##  Procedury postępowania na wypadek zagrożenia bombowego.

W przypadku otrzymania informacji o zagrożeniu bombowym należy niezwłocznie zaalarmować o tym:

*Imię nazwisko*

*Telefon*

*e-mail*

**W trakcie przyjmowania informacji o zagrożeniu bombowym należy w miarę możliwości kierować poniższymi wytycznymi:**

* Jeżeli jest to możliwe należy nagrać rozmowę w przeciwnym razie zapisać przekazaną informację.
* Staraj się podtrzymać rozmowę. Powiedz osobie telefonującej, że jesteś wdzięczny za okazaną pomoc. Pamiętaj, że osoby informujące o zamachu bombowym są często niezrównoważone psychicznie. Takie osoby zwykle oczekują uwagi i w przypadku wykazania zainteresowania można uzyskać od nich informacje dotyczące miejsc umieszczenia bomby, jej wyglądu, itp. wiadomości mogące mieć znaczenie przy przeciwdziałaniu zagrożenia.
* Poproś, aby rozmówca powtórzył wiadomość w celu upewnienia się, że informacja została zapisana lub nagrana bez błędu. Jednocześnie staraj się zapamiętać charakterystyczny sposób wymowy i akcentowania słów.
* Unikaj przerywania rozmowy i używania zwrotów w postaci: „proszę chwilę zaczekać". Takie zachowanie może spowodować wystąpienie paniki u osoby dzwoniącej oraz przerwanie rozmowy. Słuchaj uważnie dzwoniącego, zwracając uwagę na odgłosy w tle rozmowy. Zapytaj osobę dzwoniącą o nazwisko, adres i numer telefonu. W trakcie rozmowy bądź bezpośrednio po jej zakończeniu postaraj się wypełnić Kwestionariusz Przyjęcia Informacji o Sytuacji Kryzysowej stanowiący **Załącznik Nr 7.5** do niniejszego Programu.
* Osoba przyjmująca informację o zagrożeniu powinna niezwłocznie po zakończeniu rozmowy poinformować należy niezwłocznie zaalarmować o tym fakcie:
* *Imię nazwisko*
* *Telefon*
* *e-mail*
* Faktu zagrożenia nie należy rozgłaszać do momentu oceny jego realności i podjęcia decyzji o dalszych działaniach. Jednocześnie osoba, która przyjęła informację o zagrożeniu jest zobowiązana pozostać w pracy do czasu przybycia Policji i przekazać posiadane informacje.
* Dalsze postępowanie pozostaje wyłącznie w gestii Policji, która dokonuje analizy przekazanej informacji i oceny realności zagrożenia. Następnie przystępuje do działań rozpoznawczych i neutralizacyjnych W przypadku realnego zagrożenia bombowego i neutralizacji zagrożenia należy wypełnić Formularz zgłoszenia aktu bezprawnej ingerencji i przekazać go do Prezesa ULC.
* Dane kontaktowe najbliższej jednostki policji nr tel. ………..

##  Informowanie o incydentach.

W przypadku wystąpienia incydentu, naruszenia zasad lub nieprawidłowości dotyczących ochrony i bezpieczeństwa, pracownik, który był świadkiem lub sprawcą naruszenia, obowiązany jest zawiadomić swojego przełożonego, który informuje o zdarzeniu Kierownika ds. Ochrony Znanego Nadawcy lub jego zastępcę. Kierownik ds. Ochrony Znanego Nadawcy lub jego zastępcy po zakończeniu działań są zobowiązani do przesłania do Prezesa ULC formularza zgłoszenia incydentu nie później niż w ciągu 7 dni od zaistnienia zdarzenia zgodnie z Krajowym Programem Ochrony Lotnictwa Cywilnego. Informacje o zaistnieniu aktu bezprawnej ingerencji lub przygotowaniu do nich, są również niezwłocznie przekazywane do Szefa ABW.

* ABW: Tel. + 48 22 58 57 910, e-mail: cat@abw.gov.pl;
* Zespołu Monitorowania Zagrożeń ULC: tel. +48 22 520-72-60 lub +48 606-948-017, fax: +48 22 520-72-61, e-mail: zk@ulc.gov.pl.

W czasie zgłoszenia należy podać istotne dane, a w szczególności:

1. miejsce zdarzenia;
2. charakter zdarzenia;
3. swoje dane i sposób kontaktowania.

Formularz zgłoszenia aktu bezprawnej ingerencji zawarty jest w **Załączniku Nr 7.6** do niniejszego Programu.

## Wykaz załączników

7.1. Deklaracja zobowiązań.

7.2. Formularz sprawdzenia przeszłości.

7.3. Lista przedmiotów zabronionych w ładunkach lotniczych lub poczcie lotniczej.

7.4. Plan obiektu z uwzględnieniem stref dostępu i punktów dostępu.

7.5. Kwestionariusz przyjęcia informacji o sytuacji kryzysowej.

7.6. Formularz zgłoszenia aktu bezprawnej ingerencji.