



SPOŁECZNA RADA
Przeciwdziałania
Wykluczeniu i Mowie Nienawiści

NIE BĄDŹ OBOJĘTNY

Minimalny Standard Reagowania na Stygmatyzację, Wykluczenie
i Mowę Nienawiści

Praktyczny e-book wdrożeniowy dla uczelni, organizacji
pozarządowych, jednostek samorządu terytorialnego i instytucji
publicznych

Informacje o publikacji

Tytuł: Nie bądź obojętny. Minimalny Standard Reagowania na Stygmatyzację, Wykluczenie i Mowę Nienawiści

Opracowanie i wydawca: Stowarzyszenie Inicjatywa Obywatelska Pro Civium

Rekomendacja: Społeczna Rada Przeciwdziałania Wykluczeniu i Mowie Nienawiści

Projekt: „Nie wykluczam - Szanuję i Wspieram!”

ISBN wydania źródłowego: 978-83-977724-9-6

NIE WYKLUCZAM - Szanuję i Wspieram!



**FUNDUSZ
NIEOBOJĘTNYCH**
IM. MARIANA TURSKIEGO



STOWARZYSZENIE
ŻYDOWSKI INSTYTUT
HISTORYCZNY W POLSCE

Kampania społeczna. Nie bądź obojętny. Dołącz.

Charakter dokumentu

Standard jest praktycznym narzędziem organizacyjnym. Nie zastępuje przepisów prawa, procedur branżowych, obowiązków pracodawcy, uczelni, organu publicznego ani indywidualnej porady prawnej lub medycznej. Instytucja dostosowuje go do swoich kompetencji, struktury i obowiązujących regulacji.

Stan prawny i źródła internetowe zweryfikowano: 17 lipca 2026 r. Aktualność danych kontaktowych i podstaw prawnych należy sprawdzać przed użyciem.

Jak korzystać ze Standardu

Dokument został zbudowany jak instrukcja wdrożeniowa. Najpierw określa minimum organizacyjne, następnie prowadzi przez jeden algorytm obsługi każdej sprawy, a na końcu daje gotowe formularze i checklisty.

- Kierownictwo - przyjmuje Standard, wyznacza odpowiedzialność i zapewnia zasoby.
- Koordynator lub osoba kontaktowa - organizuje przyjmowanie zgłoszeń, ocenę ryzyka, dokumentację i współpracę.
- Pracownik lub wolontariusz - zna bezpieczny kanał zgłoszeń, nie prowadzi samodzielnego śledztwa i wie, kiedy uruchomić pomoc kryzysową.
- Osoba zgłaszająca - otrzymuje jasną informację, co wydarzy się ze zgłoszeniem i jakie są granice poufności.

Mapa e-booka

Część	Zakres
I. Fundament	cel, zakres, pięć filarów, pojęcia i mapa prawa
II. Minimum instytucjonalne	role, kanały zgłoszeń, poufność, dostępność i ochrona danych
III. Algorytm 8 kroków	od przyjęcia zgłoszenia do zamknięcia i monitoringu
IV. Ścieżki szczególne	internet, kryzys, zgłoszenia anonimowe i konflikty interesów
V. Wdrożenie	plan 30 dni, szkolenie, wskaźniki, oznaczenie Instytucji Przygotowanej do Reagowania
VI. Narzędzia	formularz przyjęcia, ocena ryzyka, karta sprawy, komunikaty i checklista audytowa

Zasada interpretacyjna

Najpierw bezpieczeństwo człowieka, potem formalności. Jednocześnie pomoc nie oznacza automatycznego uznania winy wskazanej osoby. Standard chroni godność, rzetelność i prawo do informacji wszystkich uczestników.

CZĘŚĆ I

Fundament Standardu

Celem Standardu jest stworzenie prostego, przewidywalnego i dostępnego systemu reagowania na stygmatyzację, dyskryminację, wykluczenie, mowę nienawiści, cyberprzemoc i przemoc psychiczną. System ma pomóc osobie, ograniczyć ryzyko i uruchomić właściwą ścieżkę - nie zastępować Policji, sądu, prokuratury, pomocy medycznej ani specjalistycznej.

Do kogo jest adresowany

- uczelnie i inne podmioty edukacyjne
- organizacje pozarządowe i podmioty ekonomii społecznej
- jednostki samorządu terytorialnego i ich jednostki organizacyjne
- instytucje publiczne, kultury, rynku pracy i pomocy społecznej
- podmioty realizujące projekty społeczne, wolontariackie i młodzieżowe

Standard obejmuje zgłoszenia osób bezpośrednio dotkniętych zdarzeniem, świadków, przedstawicieli, pracowników, wolontariuszy, uczestników działań i osób trzecich. Może zostać zastosowany także wtedy, gdy zdarzenie nie wypełnia znamion przestępstwa, lecz narusza zasady bezpieczeństwa, równego traktowania lub regulacje wewnętrzne.

Rezultat wdrożenia

Każda osoba wie, gdzie zgłosić sprawę. Każde zgłoszenie jest potwierdzone, ocenione pod kątem bezpieczeństwa, przypisane do ścieżki i udokumentowane. Nikt nie jest odsyłany bez informacji, co może zrobić dalej.

Pięć filarów

Filar	Znaczenie w praktyce
1. Nieobojętność	Zauważamy sygnał, przyjmujemy zgłoszenie i uruchamiamy ocenę. Brak pewności nie jest powodem do ignorowania.
2. Bezpieczeństwo	Najpierw oceniamy ryzyko dla życia, zdrowia i bezpieczeństwa. W kryzysie uruchamiamy służby lub pomoc specjalistyczną.
3. Szacunek	Słuchamy bez bagatelizowania, zawstydzania i wymuszania wielokrotnego opowiadania. Używamy neutralnego języka.
4. Proporcjonalność	Działanie odpowiada skali ryzyka, kompetencjom instytucji i potrzebom osoby. Nie obiecujemy rezultatu, którego nie możemy zapewnić.
5. Współpraca	Gdy sprawa wykracza poza kompetencje, organizujemy przekazanie lub konsultację, zachowując ciągłość informacji i wsparcia.

Zasady operacyjne

- poufność z granicami - informacja trafia tylko do osób, które muszą ją znać; nie obiecujemy pełnej tajemnicy, gdy prawo lub bezpieczeństwo wymagają działania
- zakaz odwetu - instytucja nie toleruje działań odwetowych wobec zgłaszającego, świadka ani osoby udzielającej pomocy
- dostępność - kanał jest zrozumiały, możliwy do użycia przez osoby z różnymi potrzebami i nie wymaga znajomości języka prawnego
- bezstronność - konflikt interesów powoduje przekazanie sprawy zastępcy lub niezależnej osobie
- ciągłość - osoba otrzymuje informację o kolejnym kroku nawet wtedy, gdy instytucja nie jest właściwa.

Pojęcia robocze

Pojęcie	Znaczenie na potrzeby Standardu
Dyskryminacja	Nierówne traktowanie związane z cechą prawnie chronioną. Zakres ochrony zależy od obszaru i właściwych przepisów.
Stygmatyzacja	Przypisywanie osobie lub grupie negatywnych etykiet lub stereotypów, które obniżają status i ograniczają udział.
Wykluczenie	Ograniczanie dostępu do edukacji, pracy, usług, relacji, uczestnictwa publicznego lub życia wspólnoty.
Mowa nienawiści	W Standardzie - komunikat wymierzony w osobę lub grupę z powodu rzeczywistej lub przypisanej cechy, który poniża, odczłowiecza, grozi, wzbudza wrogość lub nawołuje do przemocy. Ocena prawna wymaga osobnej analizy.
Cyberprzemoc	Nękanie, groźby, ośmieszanie, podszywanie się, ujawnianie danych lub rozpowszechnianie krzywdzących treści z użyciem narzędzi cyfrowych.
Wtórna wiktyimizacja	Dodatkowa krzywda powstała wskutek bagatelizowania, obwiniania, zbędnego powtarzania relacji lub niewłaściwego ujawnienia informacji.
Zgłoszenie	Informacja o zdarzeniu, które może wymagać reakcji. Zgłoszenie nie jest równoznaczne z ustaleniem odpowiedzialności.
Interwencja	Zestaw działań służących ograniczeniu ryzyka, udzieleniu informacji i wsparcia oraz uruchomieniu właściwej procedury.

Ważne rozróżnienie

Krzywdzące zachowanie może naruszać standardy etyczne, regulamin, prawo pracy, prawo cywilne lub karne - albo kilka z tych porządków jednocześnie. Osoba przyjmująca zgłoszenie nie kwalifikuje samodzielnie czynu jako przestępstwa. Jej zadaniem jest bezpieczeństwo, fakty, dokumentacja i właściwe przekierowanie.

Mapa praw i obowiązków

Standard opiera się na ochronie godności, równości, bezpieczeństwa, prywatności i dostępu do pomocy. Poniższa mapa wskazuje akty, które należy uwzględniać przy projektowaniu procedur. Nie jest zamkniętym katalogiem podstaw prawnych konkretnej sprawy.

Źródło	Znaczenie dla procedury
Konstytucja RP	art. 30 - godność; art. 32 - równość i zakaz dyskryminacji; art. 47 - ochrona życia prywatnego; art. 54 - wolność wyrażania poglądów.
Karta praw podstawowych UE	art. 1 - godność; art. 21 - zakaz dyskryminacji; art. 47 - skuteczny środek prawny.
Ustawa o równym traktowaniu	Określa obszary i sposoby przeciwdziałania naruszeniom zasady równego traktowania oraz środki ochrony.
Kodeks karny	W zależności od faktów znaczenie mogą mieć m.in. art. 119, 190, 190a, 256 i 257. Nie każde krzywdzące zachowanie wypełnia ich znamiona.
Dyrektywa 2012/29/UE	Standardy praw, wsparcia i ochrony ofiar przestępstw - m.in. informacja, szacunek, indywidualna ocena i ograniczanie wtórnej wiktymizacji.
RODO	Zasady minimalizacji, legalności, przejrzystości, bezpieczeństwa i ograniczenia przechowywania; szczególna ostrożność przy danych wrażliwych.
Akt o usługach cyfrowych	Mechanizmy zgłaszania nielegalnych treści dostawcom usług hostingu i wymogi dotyczące obsługi takich zgłoszeń.

Rzecznik Praw Obywatelskich wskazuje potrzebę działań prawnych, edukacyjnych, statystycznych i instytucjonalnych wobec mowy i przestępstw z nienawiści. Dla instytucji oznacza to, że sama deklaracja wartości nie wystarcza - potrzebne są dostępny kanał, kompetentna reakcja, dane o funkcjonowaniu systemu i regularna edukacja.

CZĘŚĆ II

Minimum instytucjonalne

	Element	Minimum
1	Decyzja kierownictwa	Formalne przyjęcie Standardu, data wejścia w życie i zakres stosowania.
2	Odpowiedzialność	Co najmniej jedna wskazana osoba kontaktowa oraz zastępstwo na czas nieobecności lub konfliktu interesów.
3	Kanał zgłoszeń	Co najmniej jeden bezpieczny, łatwy do znalezienia kanał. Zalecane są co najmniej dwa: cyfrowy i bezpośredni.
4	Algorytm	Stosowanie ośmiu kroków i czterech kategorii ryzyka A-D.
5	Dokumentacja	Chroniony rejestr, karta sprawy, zasady dostępu, retencji i usuwania.
6	Informacja	Publiczna instrukcja: gdzie zgłosić, co stanie się dalej, terminy, granice poufności, pomoc zewnętrzna.
7	Przygotowanie ludzi	Szkolenie osoby kontaktowej i podstawowy instruktaż całego zespołu.
8	Przegląd	Co najmniej raz w roku ocena skuteczności i aktualizacja danych, kanałów i procedur.

Model dla małej organizacji

Nie trzeba tworzyć nowego działu. Funkcję osoby kontaktowej może pełnić członek zarządu, koordynator projektu lub inna imiennie wyznaczona osoba. Musi jednak mieć zastępstwo, dostęp do konsultacji i bezpieczne miejsce przechowywania dokumentacji.

Role i odpowiedzialność

Rola	Odpowiedzialność
Kierownictwo	przyjmuje Standard, zapewnia zasoby, usuwa bariery, decyduje o działaniach w zakresie swoich kompetencji
Koordinator	nadzoruje wdrożenie, rejestr, terminy, szkolenia, analizę roczną i współpracę zewnętrzną
Osoba kontaktowa	przyjmuje zgłoszenie, ocenia bezpieczeństwo, ustala kategorię, informuje o ścieżkach i dokumentuje
Zastępca	przejmuje sprawę podczas nieobecności lub konfliktu interesów
IOD lub osoba ds. prywatności	pomaga ustalić podstawy, zakres, dostęp, retencję, zabezpieczenia i obsługę naruszeń danych
Pracownik lub wolontariusz	reaguje na pilne zagrożenie, zna kanał, nie obiecuje tajemnicy bez granic, nie prowadzi własnego dochodzenia
Partner zewnętrzny	udziela specjalistycznej pomocy w ramach własnych kompetencji i uzgodnionych zasad przekazania

Konflikt interesów

Sprawa musi zostać przekazana zastępcy lub osobie niezależnej, gdy dotyczy osoby kontaktowej, jej przełożonego, osoby bliskiej, podległego zespołu albo sytuacji, w której bezstronność może być rozsądnie kwestionowana. Samo odnotowanie konfliktu nie wystarcza - trzeba zmienić prowadzącego.

Kanały zgłoszeń i dostępność

Kanał powinien być widoczny na stronie WWW, dostępny bez logowania do wewnętrznego systemu i opisany prostym językiem. Nie należy wymagać od osoby zgłaszającej samodzielnej kwalifikacji prawnej ani kompletnego materiału dowodowego.

Kanał	Standard minimum
Formularz WWW	dostępny mobilnie, potwierdzenie wysłania, informacja o prywatności, możliwość opisanie potrzeb kontaktowych
E-mail	dedykowana skrzynka, ograniczony dostęp, automatyczne potwierdzenie bez ujawniania treści w temacie
Telefon	jasne godziny, możliwość oddzwonienia, procedura na wypadek kryzysu
Spotkanie	poufne miejsce, możliwość osoby wspierającej, notatka uzgodniona co do kluczowych faktów
Zgłoszenie anonimowe	przyjmowane do oceny; informacja, że anonimowość może ograniczyć możliwość wyjaśnienia i informacji zwrotnej

Komunikat przy kanale

Tekst do użycia

„Możesz zgłosić sytuację dotyczącą Ciebie lub innej osoby. Nie musisz znać przepisów ani mieć wszystkich dowodów. Potwierdzimy przyjęcie zgłoszenia nie później niż w 3 dni robocze. Najpierw sprawdzimy bezpieczeństwo i ustalimy z Tobą możliwy kolejny krok. W bezpośrednim zagrożeniu życia lub zdrowia dzwoń pod 112.”

Poufność i ochrona danych

- Minimalizacja - zbieramy tylko dane potrzebne do oceny bezpieczeństwa i prowadzenia wybranej ścieżki.
- Ograniczenie dostępu - dostęp otrzymują wyłącznie osoby z określoną rolą i rzeczywistą potrzebą.
- Bezpieczeństwo - dokumentacja nie jest przechowywana w ogólnym folderze, prywatnej skrzynce ani komunikatorze.
- Retencja - instytucja ustala okresy przechowywania dla typów spraw i bezpieczne usuwanie.
- Przejrzystość - osoba otrzymuje zrozumiałą informację o administratorze, celach, podstawach, odbiorcach i prawach.
- Dane szczególnej kategorii - informacje o zdrowiu, pochodzeniu, religii lub orientacji mogą pojawić się w sprawie; ich przetwarzanie wymaga odrębnej analizy art. 9 RODO.
- Udostępnienie na zewnątrz - przed przekazaniem sprawy ustalamy podstawę, niezbędny zakres i bezpieczny kanał. W nagłym zagrożeniu priorytetem pozostaje ochrona życia i zdrowia.

Nie obiecuj „pełnej poufności”

Na początku rozmowy wyjaśnij: kto może poznać informacje, w jakich sytuacjach instytucja będzie musiała działać i jak osoba zostanie o tym poinformowana. Poufność jest zasadą, ale nie może blokować reakcji na bezpośrednie zagrożenie ani obowiązków wynikających z prawa.

Minimalna dokumentacja bezpieczeństwa informacji

- upoważnienia i lista osób z dostępem
- rejestr dostępu lub co najmniej kontrola zmian
- zasady nazewnictwa i przechowywania plików
- kopia zapasowa i ochrona urządzeń
- procedura naruszenia ochrony danych
- harmonogram retencji i usuwania

CZĘŚĆ III

Algorytm reagowania - 8 kroków

Krok	Działanie	Minimum
1	Przyjmij	wysłuchaj, zapisz minimum, wyjaśnij zasady i potwierdź przyjęcie
2	Oceń bezpieczeństwo	sprawdź zagrożenie życia, zdrowia, eskalację i potrzeby pilne
3	Sklasyfikuj	przypisz kategorię A, B, C lub D; aktualizuj ją, gdy pojawią się nowe fakty
4	Wybierz ścieżkę	ustal cel, kompetencje, zgodę lub inną podstawę działania i potrzebnych partnerów
5	Działaj lub przekaz	udziel informacji, uruchom procedurę, zabezpiecz dowody, skonsultuj lub przekaz
6	Dokumentuj	odnotuj fakty, decyzje, podstawy, terminy, osoby odpowiedzialne i udostępnienia
7	Monitoruj	sprawdź bezpieczeństwo, wykonanie uzgodnień, odwet i potrzebę zmiany kategorii
8	Zamknij	podsumuj rezultat, poinformuj w możliwym zakresie, ustal retencję i wniosek systemowy

Dwa terminy, dwa różne cele

Do 3 dni roboczych - potwierdzenie przyjęcia i informacja o następnym kroku. Do 48 godzin - rekomendowany czas na pierwszą merytoryczną reakcję w sprawie wymagającej interwencji, o ile bezpieczeństwo nie wymaga działania natychmiast. Termin nie oznacza obowiązku zakończenia całej sprawy.

Krok 1 - przyjęcie zgłoszenia

Rozmowa pierwszego kontaktu ma zebrać minimum potrzebne do bezpieczeństwa i wyboru ścieżki. Nie jest przesłuchaniem ani postępowaniem wyjaśniającym.

Zrób

- przedstaw swoją rolę i czas rozmowy
- zapytaj, jak bezpiecznie kontaktować się z osobą
- ustal co się wydarzyło, kiedy, gdzie i czy sytuacja trwa
- zapytaj, czego osoba potrzebuje teraz
- wyjaśnij granice poufności i możliwe kolejne kroki
- zanotuj własnymi słowami tylko po uzyskaniu jasności, a kluczowe cytaty oznacz jako cytaty

Nie rób

- nie obiecuj konkretnej sankcji lub rezultatu
- nie pytaj „dlaczego wcześniej nic nie zrobiłaś/zrobiłeś”
- nie wymuszaj konfrontacji, mediacji ani kontaktu ze wskazaną osobą
- nie kopiuj całej korespondencji do szerokiego grona
- nie oceniaj wiarygodności na podstawie emocji, sposobu mówienia lub braku dokumentów

Potwierdzenie przyjęcia

Powinno zawierać: datę i identyfikator sprawy, nazwę osoby lub funkcji prowadzącej, przewidywany kolejny kontakt, informację o trybie pilnym i danych do pomocy kryzysowej. Nie umieszczaj w temacie wiadomości informacji o zdrowiu, orientacji, pochodzeniu ani opisu zdarzenia.

Krok 2 - szybka ocena bezpieczeństwa

Obszar	Pytanie kontrolne
Życie i zdrowie	Czy ktoś jest teraz ranny, w bezpośrednim niebezpieczeństwie lub nie może znaleźć bezpiecznego miejsca?
Przemoc i dostęp	Czy osoba wskazana ma teraz dostęp do osoby pokrzywdzonej, broni, narzędzia lub danych umożliwiających lokalizację?
Groźby	Czy pojawiła się konkretna groźba, termin, plan lub wcześniejsze próby realizacji?
Kryzys psychiczny	Czy występują myśli samobójcze, zamiar, plan, samouszkodzenie lub utrata kontroli?
Eskalacja	Czy zdarzenia przyspieszają, zwiększają zasięg lub obejmują kolejne osoby i kanały?
Szczególna podatność	Czy osoba jest małoletnia, zależna, izolowana, z niepełnosprawnością lub bez dostępu do bezpiecznego wsparcia?
Odwet	Czy zgłoszenie może wywołać utratę pracy, nauki, świadczenia, mieszkania, kontaktu lub dalszą przemoc?

Bezpośrednie zagrożenie

Jeżeli życie lub zdrowie jest bezpośrednio zagrożone - uruchom 112. Nie prowadź rozbudowanego wywiadu, nie pozostawiaj osoby samej, jeżeli jest to bezpieczne i możliwe, nie narażaj siebie ani innych. Punkt Reagowania nie zastępuje służb ratunkowych.

Krok 3 - klasyfikacja A-D

Kategoria	Kiedy	Reakcja
A - informacyjna	brak sygnału bezpośredniego zagrożenia; osoba potrzebuje informacji, konsultacji lub wskazania drogi	potwierdź, udziel informacji, zapisz minimum, ustal czy potrzebny kontakt kontrolny
B - interwencyjna	zdarzenie trwa lub wywołuje istotną krzywdę; potrzebne jest działanie instytucji lub partnera	ustal cel i plan, zabezpiecz dowody, uruchom procedurę, monitoruj
C - wysokie ryzyko	groźby, uporczywe nękanie, nasilony kryzys, przemoc lub szybka eskalacja bez potwierdzonego bezpośredniego zagrożenia życia	działaj pilnie, skonsultuj specjalistycznie, przygotuj plan bezpieczeństwa, rozważ służby
D - kryzys	bezpośrednie zagrożenie życia, zdrowia lub bezpieczeństwa, trwająca przemoc, próba samobójcza, ciężkie zdarzenie wymagające natychmiastowej pomocy	112 i właściwe służby; minimum pytań; bezpieczeństwo przed dokumentacją

Kategoria jest decyzją roboczą, nie diagnozą ani kwalifikacją prawną. Może zostać podwyższona lub obniżona. Każda zmiana wymaga krótkiego uzasadnienia w karcie sprawy.

Kroki 4 i 5 - wybór ścieżki i działanie

Ścieżka	Przykładowe działania
Informacyjna	wyjaśnienie możliwości, kontaktów, procedur i praw; bez pozostawiania osoby z samym linkiem
Wspierająca	rozmowa, plan bezpieczeństwa, pomoc psychologiczna, prawna, socjalna lub kryzysowa
Wewnętrzna	procedura pracownicza, studencka, etyczna, antymobbingowa, dyscyplinarna, skargowa lub bezpieczeństwa
Cyfrowa	zabezpieczenie treści, zgłoszenie platformie, ochrona kont, ograniczenie rozpowszechniania
Zewnętrzna	Punkt Reagowania, RPO, Państwowa Inspekcja Pracy, organ nadzorczy, ośrodek pomocy, Fundusz Sprawiedliwości lub inny właściwy podmiot
Prawna lub ratunkowa	Policja, prokuratura, sąd, 112, ratownictwo medyczne - zależnie od faktów i obowiązków

Test decyzji

- Czy działanie zwiększa bezpieczeństwo i odpowiada potrzebie?
- Czy mieści się w kompetencjach instytucji?
- Czy znamy podstawę przetwarzania i przekazania danych?
- Czy poinformowaliśmy osobę o możliwych skutkach i alternatywach?
- Czy istnieje ryzyko odwetu lub wtórnej wiktymizacji?
- Kto, co i do kiedy wykona?

Mediacja nie jest rozwiązaniem domyślnym

Nie proponuj jej w sytuacji przemocy, przewagi władzy, zastraszania, odwetu, braku dobrowolności lub bezpośredniego zagrożenia. Zgoda na mediację musi być świadoma i możliwa do wycofania.

Kroki 6-8 - dokumentowanie, monitoring, zamknięcie

Dokumentacja ma umożliwiać odtworzenie decyzji, a nie gromadzić wszystko „na wszelki wypadek”. Oddzielaj fakty, relacje uczestników, własne obserwacje i oceny ryzyka.

Sekcja	Co zapisać
Fakty	daty, kanały, osoby, miejsca, treści i materiały - ze wskazaniem źródła
Ocena	kategoria A-D, czynniki ryzyka i ochronne, data i osoba oceniająca
Decyzje	wybrana ścieżka, uzasadnienie, zgody lub inne podstawy, terminy i odpowiedzialność
Udostępnienia	komu, kiedy, w jakim zakresie, jakim kanałem i na jakiej podstawie przekazano dane
Monitoring	czy zagrożenie ustało, czy plan wykonano, czy pojawił się odwet, czy potrzebna jest zmiana
Zamknięcie	rezultat, informacja przekazana osobie, data, dalszy kontakt, retencja i wniosek systemowy

Warunki zamknięcia

- osiągnięto uzgodniony cel lub wykonano możliwe działania
- sprawę skutecznie przekazano właściwemu podmiotowi
- osoba otrzymała informację o dostępnych dalszych krokach
- zakończono uzgodniony monitoring
- odnotowano przyczynę, jeżeli sprawy nie można było kontynuować

Informacja zwrotna

Poufność może ograniczać zakres informacji o działaniach wobec innych osób. Nadal można przekazać: że sprawę przeanalizowano, jakie działania systemowe wykonano, gdzie uzyskać dalszą pomoc i jak wnieść zastrzeżenie do sposobu obsługi.

CZĘŚĆ IV

Ścieżka cyfrowa

W sprawach internetowych czas ma znaczenie, ponieważ treść może zostać usunięta lub szybko zwiększyć zasięg. Najpierw oceń bezpieczeństwo, potem zabezpiecz materiał w niezbędnym zakresie, a następnie zgłoś treść lub konto właściwemu usługodawcy.

Etap	Działanie
1. Zabezpiecz	pełny zrzut ekranu, URL, nazwa konta, data i godzina, kontekst wątku; oryginalne pliki, jeżeli są dostępne
2. Opisz	co jest krzywdzące, kogo dotyczy, zasięg, powtarzalność, groźby, ujawnienie danych, wpływ na bezpieczeństwo
3. Ogranicz	zmiana haseł, uwierzytelnianie wieloskładnikowe, blokady, ograniczenie widoczności danych i lokalizacji
4. Zgłoś	mechanizm platformy zgodny z jej zasadami i - w przypadku nielegalnej treści - mechanizm zgłaszania przewidziany przez akt o usługach cyfrowych
5. Monitoruj	kopie treści, nowe konta, odwet, publikacja danych, przejście do kontaktu offline
6. Eskaluj	groźby, stalking, przemoc, podszywanie się, bezprawne ujawnienie danych lub inne możliwe naruszenie prawa konsultuj specjalistycznie

Nie zwiększaj zasięgu

Nie publikuj ponownie krzywdzącej treści w komunikacie instytucji i nie wysyłaj jej do osób, które nie muszą jej znać. Do analizy używaj bezpiecznej kopii. W komunikacji publicznej opisz zjawisko i działania bez powielania materiału.

Ścieżka kryzysowa

Poziom	Działanie
D - bezpośrednie zagrożenie	112; podaj lokalizację, rodzaj zagrożenia i dostępne fakty. Pozostań w kontakcie, jeżeli jest to bezpieczne. Nie podejmuj fizycznej interwencji bez przygotowania.
C - wysokie ryzyko	pilny kontakt z osobą, konsultacja specjalistyczna, plan bezpieczeństwa, ograniczenie dostępu sprawcy, ustalenie bezpiecznego miejsca i osób wspierających
Po interwencji	zapisz fakty i decyzje, potwierdź przekazanie, zaplanuj kontakt kontrolny, zaoferuj wsparcie osobie pokrzywdzonej i osobie prowadzącej interwencję

Minimalne pytania w kryzysie

- Gdzie jesteś i czy jesteś teraz w bezpiecznym miejscu?
- Czy ktoś jest ranny lub wymaga pilnej pomocy medycznej?
- Czy osoba stanowiąca zagrożenie jest w pobliżu?
- Czy masz możliwość odejścia do bezpiecznego miejsca?
- Czy mogę wezwać pomoc i podać Twoją lokalizację?

Granica roli

Koordinators Standardu nie diagnozuje stanu zdrowia, nie prowadzi terapii i nie negocjuje samodzielnie w sytuacji bezpośredniego zagrożenia. Jego rolą jest rozpoznanie alarmu, wezwanie właściwej pomocy, przekazanie faktów i zapewnienie ciągłości wsparcia.

Zgłoszenia anonimowe, świadkowie i odwet

Zgłoszenie anonimowe należy przyjąć i ocenić. Brak danych kontaktowych może ograniczyć wyjaśnienie, ale nie zwalnia z reakcji na możliwe zagrożenie, problem systemowy lub informacje możliwe do zweryfikowania innymi źródłami.

Sytuacja	Zasada
Anonimowe	zapisz zakres możliwej weryfikacji; nie próbuj identyfikować autora bez podstawy; podejmij działania systemowe, gdy to możliwe
Od świadka	zapytaj o bezpieczeństwo osoby pokrzywdzonej i świadka; nie wymuszaj ujawnienia; ustal, co świadek widział lub słyszał bez interpretacji
Dotyczące kierownictwa	uruchom niezależnego prowadzącego i alternatywny kanał; nie przekazuj automatycznie treści osobie wskazanej
Ryzyko odwetu	zaplanuj ochronę przed zmianą grafiku, wykluczeniem, oceną, utratą roli, nękaniami i ujawnieniem danych; monitoruj po zgłoszeniu
Złośliwe lub świadomie fałszywe	oceniaj na podstawie dowodów, nie niekorzystnego wyniku sprawy; nie traktuj niepotwierdzenia jako dowodu złej wiary

Osoba wskazana w zgłoszeniu ma prawo do rzetelnej procedury, informacji w zakresie odpowiednim do etapu i możliwości przedstawienia stanowiska, jeżeli nie zagraża to bezpieczeństwu ani zabezpieczeniu materiału. Działania tymczasowe służą ograniczeniu ryzyka i nie przesądzają odpowiedzialności.

Punkt Reagowania i współpraca



Punkt Reagowania Pro Civium jest bezpieczną ścieżką pierwszego kontaktu i wsparcia dla osób oraz instytucji wdrażających Standard.

- porządkuje fakty i potrzeby
- wspiera ocenę ryzyka i wybór ścieżki
- udziela lub organizuje informacje psychologiczne i prawne w dostępnym zakresie
- pomaga w przekierowaniu do właściwej instytucji
- konsultuje stosowanie Standardu

Punkt nie zastępuje

numeru alarmowego 112, Policji, prokuratury, sądu, ratownictwa medycznego, ośrodka interwencji kryzysowej ani ustawowych obowiązków instytucji.

Kontakt: www.stopstygmatyzacji.pl | infolinia 800 201 211

CZĘŚĆ V

Plan wdrożenia - 30 dni

Termin	Rezultat
Dni 1-5	decyzja kierownictwa; właściciel wdrożenia; mapa istniejących procedur; analiza konfliktów i zasobów
Dni 6-10	osoba kontaktowa i zastępca; kanały; skrzynka i uprawnienia; zasady dostępu i retencji
Dni 11-15	lokalne ścieżki przekazania; kontakty kryzysowe; formularze; uzgodnienie z IOD i działami właściwymi
Dni 16-20	szkolenie osoby kontaktowej; ćwiczenie dwóch scenariuszy; poprawa luk
Dni 21-25	instruktaż zespołu; publikacja informacji na WWW; materiały w dostępnych formatach
Dni 26-30	test kanałów; audyt checklisty; decyzja o uruchomieniu; komunikat; data pierwszego przeglądu

Scenariusze obowiązkowego testu

- anonimowe zgłoszenie o dyskryminacji przez przełożonego
- groźby i ujawnienie danych w internecie z szybko rosnącym zasięgiem
- osoba w kryzysie psychicznym podczas rozmowy telefonicznej
- zgłoszenie dotyczące samego koordynatora

Gotowość oznacza działanie

Kanał jest uruchomiony dopiero wtedy, gdy wiadomo kto go sprawdza, jak często, kto zastępuje, gdzie trafia dokumentacja i co dzieje się poza godzinami pracy.

Szkolenie i komunikacja

Grupa	Minimum	Zakres
Wszyscy	20-30 min	jak rozpoznać alarm, gdzie przekazać zgłoszenie, czego nie obiecywać, jak nie szkodzić
Osoba kontaktowa	min. 6 h + ćwiczenia	pierwszy kontakt, ocena ryzyka, kategorie A-D, ochrona danych, dokumentacja, ścieżki zewnętrzne
Kierownictwo	60-90 min	odpowiedzialność, zasoby, konflikt interesów, odwet, decyzje i komunikacja kryzysowa
Zespół okresowo	co najmniej raz w roku	aktualizacja procedur, wnioski bez danych identyfikujących, ćwiczenie scenariusza

Informacja na stronie WWW

- nazwa Standardu i krótki cel
- przycisk lub link „Zgłoś sytuację”
- dostępne kanały i godziny
- co stanie się po zgłoszeniu i termin potwierdzenia
- granice poufności i informacja o danych osobowych
- 112 i kontakty kryzysowe
- Punkt Reagowania oraz inne źródła pomocy
- data aktualizacji informacji

Monitoring i coroczny przegląd

Obszar	Wskaźniki
Dostępność	czas odpowiedzi kanału, odsetek zgłoszeń potwierdzonych do 3 dni roboczych, dostępność alternatywnych form kontaktu
Bezpieczeństwo	odsetek spraw z udokumentowaną oceną ryzyka, liczba eskalacji C-D, czas uruchomienia pomocy
Proces	odsetek spraw z kategorią, planem, właścicielem i terminem; liczba przekazania bez potwierdzenia odbioru
Jakość	informacja zwrotna od osób, skargi na obsługę, przypadki wtórnej wiktymizacji lub odwetu
Uczenie się	szkolenia, testy kanałów, działania systemowe, zaktualizowane kontakty i procedury
Prywatność	przeglądy dostępów, usunięcia zgodnie z retencją, incydenty bezpieczeństwa informacji

Raport roczny powinien wykorzystywać dane zagregowane i nieidentyfikujące. Ma odpowiadać na pytanie, czy system działa, a nie ujawniać historie konkretnych osób. Niska liczba zgłoszeń nie musi oznaczać braku problemu - może oznaczać niewidoczny lub mało zaufany kanał.

Instytucja Przygotowana do Reagowania



Oznaczenie komunikuje, że instytucja przystąpiła do Sieci, wdrożyła Minimalny Standard Reagowania i uzyskała zgodę na używanie znaku. Samodzielne pobranie grafiki nie stanowi potwierdzenia spełnienia warunków.

Warunki użycia

- formalna decyzja o wdrożeniu
- działający kanał i wyznaczona odpowiedzialność
- przygotowanie osób realizujących Standard
- stosowanie algorytmu i dokumentacji
- publikacja informacji dla społeczności
- coroczny przegląd
- członkostwo w Ogólnopolskiej Sieci oraz autoryzacja Biura Rady

Sposób komunikowania

Używaj sformułowania „Instytucja Przygotowana do Reagowania”. Nie używaj słowa „certyfikowana”, jeżeli nie działa formalny program certyfikacji z opublikowanymi kryteriami, trybem oceny, okresem ważności i procedurą odwoławczą.

Kontakt w sprawie wdrożenia i znaku: sekretariat@stopstygmetyzacji.pl

CZĘŚĆ VI

Narzędzie 1 - karta przyjęcia zgłoszenia

Identyfikator sprawy	
Data, godzina, kanał	
Osoba przyjmująca	
Bezpieczny sposób kontaktu	
Osoba zgłaszająca	☐ osoba pokrzywdzona ☐ świadek ☐ przedstawiciel ☐ osoba trzecia ☐ anonimowo
Co się wydarzyło?	
Kiedy i gdzie?	
Czy sytuacja trwa?	☐ tak ☐ nie ☐ nie wiadomo
Czego osoba potrzebuje teraz?	
Materiały wskazane lub przekazane	
Wyjaśniono granice poufności	☐ tak ☐ nie
Przekazano informację o następnym kroku	☐ tak ☐ nie

Narzędzie 2 - szybka karta ryzyka

Czynnik	Nie	Tak	Nie wiem	Notatka
Bezpośrednie zagrożenie życia lub zdrowia	☐	☐	☐	
Trwająca przemoc albo sprawca w pobliżu	☐	☐	☐	
Konkretna groźba, plan, narzędzie lub termin	☐	☐	☐	
Myśli samobójcze, plan lub samouszkodzenie	☐	☐	☐	
Uporczywość albo szybka eskalacja	☐	☐	☐	
Ujawnienie danych lub lokalizacji	☐	☐	☐	
Szczególna zależność lub brak bezpiecznego wsparcia	☐	☐	☐	
Ryzyko odwetu	☐	☐	☐	
Potrzeba pomocy medycznej, prawnej lub kryzysowej	☐	☐	☐	

Kategoria	☐ A ☐ B ☐ C ☐ D
Uzasadnienie	
Działanie natychmiastowe	
Konsultacja lub przekazanie	
Osoba odpowiedzialna i termin	
Data ponownej oceny	

Narzędzie 3 - karta prowadzenia sprawy

Identyfikator i kategoria	
Cel uzgodniony z osobą	
Czynniki ochronne	
Wybrana ścieżka	
Działania, właściciel, termin	
Podstawa i zakres przetwarzania lub przekazania	
Materiały i miejsce przechowywania	
Monitoring - data i wynik	
Zmiana kategorii i uzasadnienie	
Rezultat i informacja zwrotna	
Data zamknięcia	
Retencja lub data przeglądu/usunięcia	

Narzędzie 4 - gotowe komunikaty

Potwierdzenie

Wzór

„Potwierdzamy przyjęcie zgłoszenia z dnia [data]. Otrzymało ono identyfikator [ID]. Sprawę prowadzi [funkcja, imię i kontakt]. Do [data] prześlemy informację o kolejnym kroku. Jeżeli sytuacja ulegnie zmianie lub pojawi się zagrożenie, skontaktuj się przez [kanał]. W bezpośrednim zagrożeniu życia lub zdrowia zadzwoń pod 112.”

Przekazanie

Wzór

„Zakres tej sprawy wykracza poza nasze kompetencje w części dotyczącej [zakres]. Możemy pomóc w kontakcie z [podmiot] i - po ustaleniu podstawy oraz zakresu danych - przekazać niezbędne informacje. Możesz też skontaktować się samodzielnie: [dane]. Ustalamy, że [kto] potwierdzi do [data], czy pomoc została uruchomiona.”

Zamknięcie

Wzór

„Zamykamy sprawę na etapie [etap], ponieważ [krótkie uzasadnienie]. Wykonano: [działania]. Nadal dostępne są: [formy pomocy]. Ze względu na poufność nie możemy przekazać wszystkich informacji dotyczących innych osób. Jeśli masz zastrzeżenia do sposobu obsługi, możesz je zgłosić przez [kanał].”

Narzędzie 5 - audyt gotowości

Lp.	Kryterium	Tak	Częściowo	Nie	Dowód / działanie
1	Standard został formalnie przyjęty i ma datę wejścia w życie.	☐	☐	☐	
2	Wyznaczono osobę kontaktową, zastępcę i ścieżkę konfliktu interesów.	☐	☐	☐	
3	Kanał zgłoszeń działa, jest testowany i widoczny na stronie WWW.	☐	☐	☐	
4	Potwierdzenie zgłoszenia następuje nie później niż w 3 dni robocze.	☐	☐	☐	
5	Stosowane są kategorie A-D i algorytm 8 kroków.	☐	☐	☐	
6	Istnieje bezpieczny rejestr, zasady dostępu, retencji i usuwania.	☐	☐	☐	
7	Osoby realizujące Standard przeszły szkolenie i ćwiczenie scenariusza.	☐	☐	☐	
8	Dostępna jest aktualna mapa pomocy kryzysowej i specjalistycznej.	☐	☐	☐	
9	Zasady poufności, ochrony danych i udostępnień są uzgodnione.	☐	☐	☐	
10	Istnieje ochrona przed odwetem i bezpieczna ścieżka spraw dotyczących kierownictwa.	☐	☐	☐	
11	Prowadzony jest monitoring jakości bez publikowania danych identyfikujących.	☐	☐	☐	
12	Ustalono datę corocznego przeglądu.	☐	☐	☐	
13	Instytucja jest członkiem Sieci i posiada autoryzację znaku, jeżeli go używa.	☐	☐	☐	

Podstawy i źródła urzędowe

1. Konstytucja Rzeczypospolitej Polskiej
<https://eli.gov.pl/eli/DU/1997/483/ogl>
2. Karta praw podstawowych Unii Europejskiej
<https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=CELEX:12012P/TXT>
3. Dyrektywa 2012/29/UE ustanawiająca normy minimalne w zakresie praw, wsparcia i ochrony ofiar przestępstw
<https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=CELEX:32012L0029>
4. Decyzja ramowa 2008/913/WSiSW w sprawie zwalczania rasizmu i ksenofobii
<https://eur-lex.europa.eu/legal-content/PL/ALL/?uri=CELEX:32008F0913>
5. Rozporządzenie (UE) 2022/2065 - akt o usługach cyfrowych
<https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=CELEX:32022R2065>
6. Rozporządzenie (UE) 2016/679 - RODO
<https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=CELEX:32016R0679>
7. Ustawa z 3 grudnia 2010 r. o wdrożeniu niektórych przepisów UE w zakresie równego traktowania - tekst jednolity
<https://eli.gov.pl/api/acts/DU/2023/970/text.html>
8. Kodeks karny - tekst jednolity ogłoszony w Dz.U. z 2025 r. poz. 383
<https://eli.gov.pl/api/acts/DU/2025/383/text/O/D20250383.pdf>
9. RPO - 20 rekomendacji dotyczących przeciwdziałania mowie nienawiści
<https://bip.brpo.gov.pl/pl/content/jak-walczyć-z-mowa-nienawisci-20-rekomendacji-rpo-dla-premiera>
10. Ministerstwo Sprawiedliwości - prawa pokrzywdzonego w postępowaniu karnym
<https://www.gov.pl/web/sprawiedliwosc/4-jakie-pokrzywdzony-ma-prawa-i-obowiazki-w-postepowaniu-karnym>
11. Fundusz Sprawiedliwości - aktualna sieć pomocy osobom pokrzywdzonym przestępstwem
<https://www.funduszsprawiedliwosci.gov.pl/pl/znajdz-osrodek-pomocy/>

Zasada aktualności

Przed wdrożeniem i podczas corocznego przeglądu instytucja sprawdza aktualne brzmienie przepisów, dane kontaktowe i właściwość podmiotów. W sprawach indywidualnych korzysta z pomocy osoby posiadającej odpowiednie kompetencje prawne, medyczne lub psychologiczne.



NIE BĄDŹ OBOJĘTNY

Reagowanie zaczyna się od zauważenia, bezpiecznego przyjęcia informacji i wykonania właściwego następnego kroku.

www.stopstygmatyzacji.pl

Infolinia Punktu Reagowania: 800 201 211

sekretariat@stopstygmatyzacji.pl

Stowarzyszenie Inicjatywa Obywatelska Pro Civium

Społeczna Rada Przeciwdziałania Wykluczeniu i Mowie Nienawiści