Standardy ochrony dzieci

Wytyczne

Jak stworzyć standardy ochrony dzieci

Ochrona dziecka w Internecie

Spis treści

Do czego służą te wytyczne

Przygotowaliśmy te wytyczne, żeby ułatwić Ci pracę nad standardami ochrony dzieci w Internecie dla Twojej placówki.

To szczegółowe wskazówki, które są rozwinięciem ogólnych wytycznych do standardów ochrony dzieci. W tych wytycznych radzimy, jak możesz opisać:

- rodzaje zagrożeń, które związane są z Internetem i nowymi technologiami,
- dodatkowe zasady interwencji w przypadku wystąpienia takich zdarzeń,
- rolę i zadania **koordynatora bezpieczeństwa w sieci**,
- zabezpieczenia sieci i urządzeń,
- działania edukacyjne związane z bezpieczeństwem w Internecie.

Rodzaje zagrożeń w Internecie

Zagrożenia dla bezpieczeństwa dzieci w Internecie stale się rozwijają. Oznacza to, że nie da się wypisać wszystkich potencjalnych zagrożeń. Poniżej przedstawiamy jedynie przykłady takich sytuacji.

W Twoim dokumencie standardów ochrony dzieci wskaż i opisz te zagrożenia, na które mogą być narażone dzieci w Twojej placówce. Poniżej opisaliśmy przykłady tych zagrożeń.

Niedozwolone zachowania między dziećmi

Dzieci mogą być narażone na przemoc ze strony innych dzieci. Często dzieje się to z wykorzystaniem technologii, na przykład Internetu czy smartfonów.

Przykłady takich zachowań między dziećmi to:

- nękanie;
- straszenie;
- szantażowanie;
- podszywanie się pod kogoś – np. kradzież zdjęć z mediów społecznościowych i zakładanie fałszywych profili w aplikacjach randkowych;
- przesyłanie i udostępnianie ośmieszających, kompromitujących informacji, zdjęć czy filmów.

Przemoc seksualna z wykorzystaniem wizerunku dziecka

Dzieci mogą być pokrzywdzone przemocą seksualną, w której wykorzystywany jest ich wizerunek. Chodzi na przykład o:

- robienie filmów i zdjęć z nagimi dziećmi lub dziećmi w trakcie czynności seksualnej – szczególnie przy użyciu przemocy, groźby lub podstępu;
- rozpowszechnianie takich materiałów;

- tworzenie takich materiałów przy użyciu sztucznej inteligencji (*deepfake*).

Dostęp do nielegalnych treści

Dzieci mogą mieć dostęp do treści, których rozpowszechniania zabrania prawo, na przykład do:

- materiałów przedstawiających seksualne wykorzystanie dziecka [1] (*CSAM*);
- twardej pornografii[2] – prezentującej przemoc lub wykorzystywanie zwierząt;
- materiałów promujących rasizm i ksenofobię[3] – faszystowski lub inny totalitarny ustrój państwa oraz nienawiść ze względu na narodowość, pochodzenie etniczne, rasowe, wyznanie lub brak wyznania;
- materiałów propagujących lub pochwalających zachowania o charakterze pedofilskim[4];
- filmów i zdjęć z nagimi osobami lub osobami w trakcie czynności seksualnej; wykonanych przy użyciu przemocy, groźby, podstępu lub udostępnianych bez zgody tej osoby[5];
- treści, które zawierają uwodzenie dziecka poniżej 15 r.ż. przez Internet (*child grooming*)[6];
- szantażu na tle seksualnym;

Dostęp do szkodliwych treści

Dzieci mogą mieć dostęp do treści nieodpowiednich do ich wieku – na przykład takich, które zawierają:

- obrazy przemocy i śmierci;
- inne drastyczne sceny;

[1] Art. 202 § 3, § 4, §4a, §4b Kodeksu karnego
[2] Art. 202 § 3 Kodeksu karnego
[3] Art. 256 Kodeksu karnego
[4] Art. 200b Kodeksu karnego
[5] Art. 191a Kodeksu karnego
[6] Art. 200a Kodeksu karnego

- pornografię;
- okrucieństwo wobec zwierząt;
- nawołania do samookaleczeń, samobójstw;
- promowanie szkodliwych substancji, nawet jeśli nie są one wprost nazwane narkotykami;
- promowanie niebezpiecznych postaw (na przykład pro-ana) czy wyzwań online;
- zachęty do wstąpienia do radykalnych ruchów lub sekt;
- zachęty do przemocy i przestępstw;
- dyskryminację;
- degenerację (np. patostreamy).

Dostęp do nieodpowiednich kontaktów i usług online

Dzieci mogą być narażone na kontakty, które są przejawem:

- presji ze strony rówieśników;
- groomingu;
- cyberprzemocy;
- sextingu;
- szantażu na tle seksualnym.

Dzieci mogą też mieć dostęp do nieodpowiednich dla nich narzędzi i platform społecznościowych, na przykład takich, które:

- umożliwiają zarabianie na aktywności seksualnej dzieci;
- organizują gry hazardowe online;
- prezentują reklamy niedostosowane do wieku dzieci.

Dodatkowe zasady interwencji

Jeśli w Twojej placówce mogą mieć miejsce zdarzenia związane z zagrożeniami w Internecie – opisz dodatkowe zasady interwencji w takich przypadkach.

Dowody

W standardzie opisz, jak Twoja placówka będzie zbierać i zabezpieczać dowody w zdarzeniach związanych z zagrożeniami w Internecie. Mogą to być:

- wiadomości email;
- SMS-y i MMS-y;
- listy połączeń telefonicznych;
- wiadomości głosowe;
- kopie treści rozmów w komunikatorach i czatach;
- zrzuty ekranu wpisów na stronach internetowych, komentarzy lub zdjęć w serwisach społecznościowych.

Gdy będziesz ustalać zasady zbierana tych dowodów – pamiętaj o poszanowaniu praw dziecka, w tym prawa do prywatności.

Określ również sposób opisywania tych dowodów, co ułatwi dalsze postępowanie. Opis powinien zawierać:

- datę otrzymania;
- dane nadawcy – nazwę użytkownika, adres wiadomości email, numer telefonu;
- adres strony internetowej lub nazwę profilu w mediach społecznościowych.

Jeśli dowody wskazują, że zostało naruszone prawo – placówka już w tym momencie powinna powiadomić Policję.

Usunięcie materiałów

W standardzie opisz, w jaki sposób Twoja placówka będzie wspierać opiekunów w usuwaniu nielegalnych, kompromitujących lub krzywdzących materiałów z Internetu.

Opiekunowie powinni dowiedzieć się, że mogą to zrobić:

- we współpracy z zespołem Dyżurnet.pl – ekspertami Naukowej i Akademickiej Sieci Komputerowej – Państwowy Instytut Badawczy;

- samodzielnie, przez odpowiedni formularz na stronie serwisu, w którym znalazły się takie materiały.

Dodatkowego wsparcia może udzielić telefon zaufania:

- dla dzieci i młodzieży – 116 111
- dla rodziców i nauczycieli – 800 100 100

Podobne materiały mogą być również widoczne w wynikach wyszukiwarek internetowych, na przykład Google. W takim przypadku można skorzystać z prawa do bycia zapomnianym, które wynika z unijnego rozporządzenia.

Jeśli w sieci znajdują się materiały intymne opublikowane bez zgody danej osoby, w usunięciu ich pomóc mogą również rozwiązania na stronie:

- takeitdown.ncmec.org[7]
- stopncii.org

Monitoring po interwencji

W standardzie opisz, w jaki sposób Twoja placówka będzie monitorować rozwój zdarzenia również po jego przerwaniu. Możesz na przykład opisać kto i w jaki sposób będzie kontrolował, czy dzieci, które uczestniczyły w tym wydarzeniu (jako osoby pokrzywdzone, sprawcy lub świadkowie), nie są pokrzywdzone dalszą przemocą, na przykład wyśmiewaniem. Opisz również działania, które kierownik i zespół placówki powinien zaplanować, żeby uniknąć podobnych zdarzeń w przyszłości. Zaplanuj ocenę tych działań z dłuższej perspektywy.

Rola koordynatora bezpieczeństwa w sieci

W standardzie opisz kompetencje i obowiązki **koordynatora bezpieczeństwa w sieci**. To osoba, która odpowiada za techniczne i organizacyjne przygotowanie Twojej placówki do

[7]Planowane jest udostępnienie tego rozwiązania w języku polskim, więc nazwa strony internetowej może się zmienić.

zapewnienia bezpiecznych warunków korzystania przez dziecko z sieci teleinformatycznych, w tym Internetu, na terenie placówki.

Skonsultuj wszystkie części standardu, które dotyczą bezpieczeństwa w Internecie, z koordynatorem w Twojej placówce. Dotyczy to przede wszystkim zapisów związanych z zabezpieczeniem sieci i urządzeń w placówce.

Koordynatora bezpieczeństwa w sieci wyznacza kierownik placówki. Koordynatorem powinna zostać osoba, która:

- ma odpowiednie kompetencje techniczne – potrafi wprowadzić zabezpieczenia informatyczne chroniące przed nielegalnymi i szkodliwymi treściami;
- rozumie cyfrową rzeczywistość – zna zagrożenia technologiczne i społeczne oraz wie, jak dzieci wykorzystują Internet i technologie;
- regularnie szkoli się w zakresie reagowania na incydenty, na przykład na przemoc z użyciem technologii;
- potrafi wykorzystywać rozwiązania online w edukacji;
- zna zasady prostej i efektywnej komunikacji – potrafi dostosować język i formę informacji do potrzeb odbiorcy.

Zabezpieczenie sieci

Blokada niebezpiecznych treści

Jeśli Twoja placówka zapewnia dzieciom dostęp do Internetu – koordynator bezpieczeństwa w sieci musi wprowadzić rozwiązania, które zablokują nielegalne i szkodliwe treści.

W standardzie opisz:

- jakie treści powinny być zablokowane;

  Blokady powinny dotyczyć tylko treści niebezpiecznych. Nie powinny wprowadzać nadmiernych ograniczeń w dostępie do zasobów internetowych. Weź uwagę wiek dzieci, specjalne potrzeby, język,

niepełnosprawności i neuroróżnorodność.
Jednym z zadań placówki powinno być edukowanie dzieci w zakresie bezpiecznego korzystania z Internetu. Nadmierne ograniczenia mogą spowodować, że dzieci nie zdobędą takich umiejętności.

- konkretne oprogramowanie i funkcje – programy antywirusowe, narzędzia ochrony rodzicielskiej oraz monitorowania aktywności użytkowników, tryby bezpiecznego wyszukiwania (np. SafeSearch w Google);
- zasady instalacji i aktualizacji tego oprogramowania – najlepiej przynajmniej raz w miesiącu;
- zasady sprawdzania, czy oprogramowanie i zakres blokowanych treści odpowiada potrzebom dzieci i zmieniającym się zagrożeniem w Internecie – najlepiej co najmniej raz w roku.

Oprogramowanie, które wskazujesz w standardzie, powinno:

- pochodzić od sprawdzonego, godnego zaufania dostawcy – koordynator bezpieczeństwa w sieci sprawdza praktyki bezpieczeństwa, certyfikaty, historię firmy, recenzje i opinie użytkowników i ekspertów;
- oferować mechanizmy szyfrowania danych, szczególnie jeśli będą w nim przetwarzane dane wrażliwe;
- być regularnie aktualizowane przez dostawcę;
- być wspierane przez dostawcę – najlepiej, by dostawca umożliwiał zgłaszanie błędów i incydentów bezpieczeństwa oraz szybko na nie reagował;
- mieć dostępną politykę prywatności zgodną z obowiązującym prawem, na przykład RODO;
- mieć mechanizmy regularnego tworzenia kopii zapasowych (backupu).

Jeśli oprogramowanie będzie integrowane (łączone) z innymi systemami w placówce – integracje powinny być bezpieczne i zgodne ze standardami.

Zalecamy, by placówki oświatowe korzystały z Ogólnopolskiej Sieci Edukacyjnej (OSE) oraz z zaawansowanych usług bezpieczeństwa OSE plus.

Konfiguracja sieci wifi

Jeśli placówka korzysta z sieci wifi, w standardzie opisz zasady konfiguracji tej sieci.

Koordynator bezpieczeństwa w sieci w Twojej placówce powinien:

- zabezpieczyć sieć silnymi hasłami;
- zmienić domyślne hasła administratora w routerach;
- wyłączyć opcję zdalnego dostępu do routera;
- regularnie aktualizować oprogramowanie routera – jeśli to możliwe, przy pomocy automatycznej aktualizacji;
- korzystać ze standardu WPA3 w routerze lub – jeśli nie wszystkie urządzenia w sieci obsługują najnowsze protokołu – ustawić poziom zabezpieczeń łączący dwa protokoły (na przykład WPA2/WPA3);
- włączyć WPS (Wifi Protected Setup) – funkcję routerów bezprzewodowych, która umożliwia łączenie urządzeń z siecią po naciśnięciu przycisku na routerze;
- cyklicznie sprawdzać listę urządzeń podłączonych do sieci placówki i blokować nieznane urządzenia;
- skonfigurować DNS[8] w routerze tak, by DNS-y blokowały domeny z nieodpowiednimi treściami[9]. – dzięki temu wszystkie urządzenia w sieci nie będą mogły łączyć się z takimi domenami.

Dostęp do sieci przez prywatne urządzenia

W standardzie opisz zasady, na jakich dzieci mogą używać prywatnych urządzeń w placówce.

[8] W przypadku korzystania z OSE nie jest to konieczne.
[9] Na przykład Cloudflare w wersji „Family" które oprócz stron z pornografią blokują także strony ze złośliwym oprogramowaniem: 1.1.1.3 oraz 1.0.0.3.

Jeśli Twoja placówka chce zapewnić dostęp do swojej sieci wifi również z prywatnych urządzeń dzieci, w standardzie opisz również zasady używania takiej sieci.

Koordynator bezpieczeństwa w sieci w Twojej placówce powinien:

- wydzielić zamkniętą, zabezpieczoną silnym hasłem sieć dla urządzeń spoza placówki;
- przygotować regulamin bezpiecznego korzystania z tej sieci;
- wprowadzić wymóg akceptacji regulaminu przed przyłączeniem urządzenia do sieci.

Twoja placówka nie może brać odpowiedzialności za zabezpieczenia prywatnych urządzeń.

Dzieci mogą korzystać z dostępu do Internetu z prywatnych urządzeń. Twoja placówka powinna promować dobre praktyki i bezpieczne zachowania również w takich przypadkach.

Zabezpieczenie urządzeń

Używanie urządzeń placówki

W standardzie opisz zasady, na jakich dzieci mogą korzystać z urządzeń, które należą do Twojej placówki.

Urządzenia placówki powinny być podłączone do Internetu wyłącznie przez sieć tej placówki. Dzieci nie powinny podłączać tych urządzeń do innych sieci, na przykład publicznych sieci wifi albo osobistych hotspotów.

Uprawnienia do urządzeń i programów

W standardzie opisz, na jakich zasadach Twoja placówka nadaje dostępy do urządzeń i oprogramowania dla dzieci i innych użytkowników, na przykład pracowników placówki.

Jeśli to możliwe, zalecamy, by każdy użytkownik miał własne konto i hasło użytkownika.

Dzieci powinny korzystać z kont o takich uprawnieniach, które są im potrzebne na co dzień. Nie powinny mieć dostępu do kont administracyjnych – te powinny być utworzone tylko dla pracowników, którzy potrzebują ich do swoich zadań.

Zabezpieczenie urządzeń placówki

W standardzie opisz, w jaki sposób koordynator bezpieczeństwa w sieci w Twojej placówce będzie:

- oznaczać urządzenia, które należą do Twojej placówki, prowadzić ich rejestr i zabezpieczać je przed kradzieżą;
- ograniczyć dostęp od pomieszczeń z urządzeniami, z których nie będą korzystać dzieci;
- aktualizować systemy operacyjne urządzeń – najlepiej co najmniej raz w miesiącu.
- sprawdzać, czy na urządzeniach placówki nie znajdują się nielegalne, szkodliwe i nieodpowiednie dla dzieci treści – najlepiej co najmniej raz w miesiącu.

Zabezpieczenie danych

W standardzie opisz rozwiązania, które umożliwią szyfrowanie danych wrażliwych na urządzeniach Twojej placówki – na przykład danych osobowych uczniów, rodzin i pracowników placówki.

Edukacja

W standardzie opisz działania, które mogą pomóc rozwijać wiedzę i świadomość o zagrożeniach w Internecie. Kierownik Twojej placówki powinien zaplanować działania edukacyjne przy wsparciu koordynatora bezpieczeństwa w sieci.

Zasady bezpieczeństwa dla osób, które korzystają z Internetu

Dziecko, które korzysta z Internetu, powinno wcześniej poznać zasady bezpieczeństwa w Internecie. Odpowiada za to koordynator bezpieczeństwa w sieci w Twoje placówce. W standardzie opisz, w jaki sposób koordynator:

- opracuje zbiór zasad bezpiecznego korzystania z Internetu;
- przedstawi te zasady dzieciom, ich rodzicom i opiekunom oraz zespołowi placówki;
- będzie cyklicznie spotykać się z dziećmi i rozmawiać z nimi o zasadach bezpieczeństwa w Internecie – najlepiej co najmniej raz w semestrze;
- przygotuje jednostronicową informację na temat zagrożeń i rozwiązań, które zapewniają bezpieczeństwo w Internecie dla rodziców i opiekunów;
- będzie na bieżąco informować wszystkie osoby, które korzystają z Internetu w placówce, o zmianach w zasadach bezpieczeństwa i regulaminach.

Zakres tych zasad i sposób ich przedstawienia musi być dostosowany do wieku i potrzeb dzieci. Koordynator powinien wziąć pod uwagę różne urządzenia (na przykład laptopy, tablety, smartwatche, drukarki, skanery, kamery internetowe, monitory) i sposoby ich wykorzystywania, w tym w ramach nauki zdalnej.

Polecamy materiały edukacyjne na temat bezpieczeństwa online na stronach gov.pl: Materiały do CYBER lekcji.

W standardzie opisz też, gdzie i w jaki sposób dzieci i rodzice będą mieć stały dostęp do materiałów o bezpieczeństwie w sieci – na przykład na stronie internetowej placówki.

Rozwój kompetencji dzieci

W standardzie opisz sposoby na rozwój innych, powiązanych kompetencji u dzieci. Poza wiedzą o zagrożeniach w Internecie, dzieci powinny rozwijać również:

- krytyczne myślenie;
- miękkie kompetencje w obszarze komunikacji i emocji;
- zdolność aktywnego poszukiwania pomocy;

- świadomość znaczenia cyfrowej równowagi (digital wellbeing);
- wiedzę na temat innych zagrożeń prywatności.

Współpraca z rodzicami i opiekunami

W standardzie opisz zasady, zgodnie z którymi Twoja placówka:

- wskaże rodzicom i opiekunom narzędzia kontroli rodzicielskiej;
- będzie informować – na przykład podczas zebrań z rodzicami – dlaczego i jak z nich korzystać.

Polecamy bezpłatną aplikację dla rodziców, dostępną na smartfony, tablety i komputery: mOchrona – aplikacja ochrony rodzicielskiej

Polityka bezpieczeństwa

W standardzie określ, kto odpowiada za politykę bezpieczeństwa informatycznego placówki i gdzie jest ona opublikowana.

Aktualizacja standardu

W standardzie opisz zasady i częstotliwość przeglądu i aktualizacji standardu Twojej placówki. Przy każdym przeglądzie weź pod uwagę:

- zmiany w Internecie i technologiach;
- ogólną sytuację i politykę placówki;
- zadania koordynatora bezpieczeństwa w sieci;
- wiedzę i kompetencję personelu placówki;
- podstawę programową;
- aktualność i skuteczność rozwiązań technologicznych;
- opinie ze strony personelu, dzieci i ich rodziców i opiekunów.

Określ też zasady ewaluację oprogramowania, która powinna być wykonywana przynajmniej raz w roku lub zawsze, gdy:

- pojawi się nowe ryzyko lub zagrożenie;
- zostanie wprowadzana nowa technologia;
- zmieni się sposób działalności placówki.