**Uwaga, to ważne!**

Ten dokument to materiał pomocniczy, jest jedynie podpowiedzią. Nie zawiera wszystkich zasad, a niektóre z nich mogą nie być przydatne w danej instytucji.

**Wytyczne do standardów ochrony** **dzieci**

**Ochrona dziecka w Internecie**

**Wersja rozbudowana**

Spis treści

[I. Relacje między dziećmi – elementy istotne dla obszaru bezpieczeństwa w cyberprzestrzeni 2](#_Toc168483883)

[II. Korzystanie z Internetu i urządzeń mobilnych 2](#_Toc168483884)

[III. Obowiązki koordynatora bezpieczeństwa w sieci 9](#_Toc168483885)

[IV. Przegląd zasad korzystania z Internetu i urządzeń mobilnych 10](#_Toc168483886)

[V. Praktyczne informacje (Załącznik) 10](#_Toc168483887)

Poniżej prezentujemy sugerowane wytyczne do wykorzystania przy pracach nad standardami ochrony dzieci w zakresie obszaru bezpieczeństwa w cyberprzestrzeni.

Wytyczne zostały opracowane z myślą o szkołach, nie będą więc mogły zostać wykorzystane w  każdej placówce, instytucji, czy też w każdym rodzaju działalności. Mogą one natomiast stanowić podpowiedź, przy czym zawsze standardy należy tworzyć w sposób dostosowany do charakteru i rodzaju placówki, instytucji lub działalności. Muszą one uwzględniać typ/rodzaj placówki, instytucji lub działalności, a co za tym idzie - jej potrzeby i możliwości wynikające z ogólnych zasad i celu funkcjonowania.

**Termin ważny przy tworzeniu standardów dla obszaru bezpieczeństwa w cyberprzestrzeni**

**Koordynator bezpieczeństwa w sieci** – pracownik wyznaczony przez kierownictwo placówki, odpowiedzialny za zapewnienie bezpiecznych warunków korzystania przez dziecko z sieci teleinformatycznych, w tym Internetu, na terenie placówki.

### I. Relacje między dziećmi – elementy istotne dla obszaru bezpieczeństwa w cyberprzestrzeni

**Zachowania niedozwolone obejmują**:

Każdą formę przemocy z wykorzystaniem technologii informacyjnych i komunikacyjnych (np. Internet, telefon komórkowy), występującą najczęściej w formie nękania, straszenia, szantażowania, podszywania się w sieci pod kogoś wbrew jego woli, przesyłania oraz udostępniania materiałów pornograficznych, zwłaszcza związanych z prezentowaniem przemocy lub posługiwaniem się zwierzęciem, publikowania lub rozsyłania ośmieszających, kompromitujących informacji, zdjęć, filmów,

Każdą formę przemocy seksualnej z wykorzystaniem wizerunku, występującą najczęściej w formie utrwalania wizerunku nagiej osoby lub osoby w trakcie czynności seksualnej, zwłaszcza używając w tym celu przemocy, groźby bezprawnej lub podstępu wobec niej albo rozpowszechniania takich wizerunków bez jej zgody (włączając materiały wytworzone i przetworzone przez osobę widoczną na materiale oraz powstałe z wykorzystaniem sztucznej inteligencji),

### II. Korzystanie z Internetu i urządzeń mobilnych

**Przegląd zagrożeń**

Zagrożenia dla bezpieczeństwa dzieci online stale się rozwijają, ale możliwe jest wskazanie ich otwartego katalogu sygnalizując, na co w pierwszej kolejności należy zwrócić uwagę. Poniżej przedstawiono przykłady zagrożeń.

**Narażenie na treści nielegalne**

Do treści nielegalnych zalicza się m.in.:

* materiały przedstawiające seksualne wykorzystanie dziecka[[1]](#footnote-1) – prawo polskie zabrania produkowania, utrwalania, sprowadzania, rozpowszechniania, prezentowania, przechowywania, uzyskiwania dostępu oraz posiadania treści pornograficznych z udziałem dziecka;
* materiały przedstawiające twardą pornografię[[2]](#footnote-2) – prawo polskie zabrania rozpowszechniania i publicznego prezentowania pornografii związanej z wykorzystaniem przemocy lub posługiwaniem się zwierzęciem;
* treści propagujące rasizm i ksenofobię[[3]](#footnote-3) – polskie prawo zabrania propagowania faszystowskiego lub innego totalitarnego ustroju państwa oraz nawoływania do nienawiści na tle różnic narodowościowych, etnicznych, rasowych, wyznaniowych lub ze względu na bezwyznaniowość;
* inne nielegalne treści – treści nie dotyczące żadnej z powyższych kategorii, ale skierowane przeciwko bezpieczeństwu dzieci, na przykład: propagowanie lub pochwalanie zachowań o charakterze pedofilskim[[4]](#footnote-4), materiały utrwalające wizerunek nagiej osoby lub osoby w trakcie czynności seksualnej przy użyciu przemocy, groźby bezprawnej lub podstępu albo rozpowszechniane bez jej zgody[[5]](#footnote-5), treści pornograficzne udostępniane dziecku [[6]](#footnote-6), uwodzenie dziecka poniżej 15 r.ż. przez Internet, tzw. child grooming[[7]](#footnote-7), zjawisko szantażu na tle seksualnym (określane również jako „sextortion”).

**Narażenie na treści szkodliwe i nieodpowiednie do wieku**

Do treści szkodliwych i nieodpowiednich zalicza się m.in. treści obrazujące przemoc, obrażenia fizyczne, prezentujące drastyczne sceny, śmierć, okrucieństwo wobec zwierząt, treści nawołujące do podejmowania działań autodestrukcyjnych (samookaleczeń, pro-ana, samobójstw, zażywania szkodliwych substancji, w tym środków psychoaktywnych niezidentyfikowanych jednoznacznie jako narkotyki itp.), treści nawołujące do przemocy, przestępczości, radykalizacji (również sekty) i ekstremizmu, patostreamy, treści dyskryminacyjne oraz pornograficzne.

**Narażenie na szkodliwe i nieodpowiednie kontakty online oraz usługi online**

Do zachowań takich zalicza się m.in. presję rówieśniczą, cyberprzemoc, grooming, szantaż na tle seksualnym, aktywność seksualną jako źródło dochodu osób nieletnich, hazard online, reklamy niedostosowane do wieku, media społecznościowe niedostosowane do wieku.

**Narażenie na szkodliwe i ryzykowne zachowania**

Do zachowań takich zalicza się m.in. podejmowanie wyzwań online, seksting, wywieranie presji, stosowanie przemocy z wykorzystaniem technologii informacyjnych i komunikacyjnych.

**Działania w celu bezpiecznego korzystania z Internetu i urządzeń mobilnych**

1. **Placówka**, zapewniając dzieciom dostęp do Internetu za pomocą własnej sieci wifi (lub w inny sposób), jest zobowiązana podejmować działania, które zablokują dostęp do treści nielegalnych, szkodliwych i nieodpowiednich dla dziecka. W tym celu należy:

* ustalić zakres zabezpieczenia oraz blokowania dostępu do treści nielegalnych, szkodliwych i nieodpowiednich dla dzieci;
* dokonać wyboru konkretnego oprogramowania (w tym np. oprogramowania antywirusowego, narzędzia ochrony rodzicielskiej, monitorowania aktywności użytkowników itp.);
* zainstalować oprogramowanie zabezpieczające oraz blokujące;
* dokonywać bieżącej aktualizacji oprogramowania, o którym mowa w pkt 3;
* przed dopuszczeniem urządzeń osobistych do sieci wifi placówki, wydzielić sieć zamkniętą z hasłem oraz wymóg akceptacji regulaminu przed przyłączeniem urządzenia;

**Uwaga: Zaleca się korzystanie przez placówki oświatowe z Ogólnopolskiej Sieci Edukacyjnej (OSE) oraz, w jej ramach, z zaawansowanych usług bezpieczeństwa OSE plus.**

2. **Dziecko** może korzystać z dostępu do Internetu na urządzeniu placówki wyłącznie przy wykorzystaniu sieci tej placówki. Zwraca się szczególną uwagę, aby przyjęte środki bezpieczeństwa nie prowadziły do nieuzasadnionych ograniczeń w dostępie do zasobów internetowych. Nadmierne blokowanie może negatywnie wpłynąć na rozwijanie zdolności bezpiecznego korzystania z Internetu wśród dzieci. W zakresie urządzeń osobistych placówka promuje dobre praktyki.

3. **Infrastruktura** sieciowa placówki umożliwia dostęp do Internetu personelowi placówki oraz dzieciom na zasadach szczegółowo określonych w zasadach bezpiecznego korzystania z Internetu, z zachowaniem poniższych zasad.

4. Działania, które należy podjąć w sytuacji ujawnienia na urządzeniu placówki treści szkodliwych i nieodpowiednich do wieku dzieci szczegółowo reguluje procedura interwencji.

5. Warunkiem dopuszczenia dziecka do korzystania z urządzeń placówki jest zapoznanie się przez to dziecko z zasadami bezpiecznego korzystania z Internetu. Dokłada się starań, aby proces zapoznania był efektywny i odpowiadał potrzebom dzieci.

6. Niezależnie od obowiązku, o którym mowa w ustępie 3, placówka zapewnia stały dostęp do materiałów edukacyjnych, dotyczących zasad bezpiecznego korzystania z Internetu (np. poprzez zamieszczanie ich na stronie internetowej, udostępnianie rodzicom i dzieciom itp.)

**Procedura interwencji**

W przypadku ujawnienia treści nielegalnych, szkodliwych lub nieodpowiednich do wieku, lub w przypadku zdarzeń godzących w bezpieczeństwo dzieci związanych z korzystaniem z Internetu (np. nieodpowiednie kontakty, ryzykowne zachowania itd.) należy podjąć następujące działania:

1. **Działania wobec aktu/zdarzenia – opis przypadku, ustalenie okoliczności zdarzenia, zabezpieczenie dowodów oraz monitoring pointerwencyjny:**

a) Każde zgłoszenie/ przypadek ujawnienia treści szkodliwych lub nieodpowiednich do wieku powinno zostać zarejestrowane, przenalizowane oraz odpowiednio udokumentowane. W analizie zdarzenia powinien znaleźć się dokładny opis zdarzenia, wskazanie osób uczestniczących i/lub podjętych działań w celu identyfikacji sprawcy oraz materiały dokumentujące zdarzenie. Dowodem mogą być np.: wiadomości e-mailowe, SMS-y i MMS-y, historia połączeń w telefonie komórkowym, wiadomości nagrane na pocztę głosową telefonu komórkowego, zrzuty ekranu prezentujące wpisy na stronach internetowych, komentarze do wpisów lub zdjęć w serwisach społecznościowych, blogach, zdjęcia, grafiki, treści rozmów prowadzonych przy użyciu komunikatorów lub czatów. Zabezpieczenie tych dowodów powinno się odbywać z poszanowaniem praw dziecka, w tym prawa do prywatności.

b) Dowody powinny zostać zabezpieczone i opisane (data otrzymania, treść wiadomości, dane nadawcy tj. nazwa użytkownika, adres email, adres strony WWW). Właściwe opisanie dowodów ułatwia dalsze postępowanie, szczególnie w sytuacji naruszenia prawa. Jeśli zebrane dowody wskazują na naruszenie prawa należy niezwłocznie powiadomić Policję i przekazać jej cały zgromadzony materiał dowodowy. W celu usunięcia z Internetu nielegalnych, kompromitujących lub krzywdzących materiałów należy poinformować rodziców/opiekunów h o możliwościach ich usunięcia we współpracy z Dyżurnet.pl oraz o trybie zgłaszania takich treści poprzez formularz na stronie, na której materiał został opublikowany. Dodatkową pomocą mogą służyć (telefony zaufania: 116 111 dla młodzieży i dzieci oraz 800 100 100 dla rodziców i nauczycieli). Pamiętać należy o prawie do bycia zapomnianym wynikającym z unijnego rozporządzenia o ochronie danych osobowych gwarantującym w uzasadnionych przypadkach usunięcie konkretnych linków z wyszukiwarki Google, w związku z czym nie będą mogły być wyszukane przy wpisywaniu jakiejkolwiek frazy. Możliwe jest również skorzystanie ze stron: https://takeitdown.ncmec.org/ oraz <https://stopncii.org/>, pomagających usunąć z Internetu materiały intymne z wizerunkiem osoby, która nie wyraziła zgody na upublicznienie treści.

c) Monitoring pointerwencyjny. Niezwykle istotnym elementem procedury interwencyjnej jest systematyczne prowadzenie monitoringu zdarzenia po jego przerwaniu i zastosowaniu środków naprawczych. W praktyce oznacza to przede wszystkim regularne pozyskiwanie informacji na temat sytuacji, potrzeb uczestników incydentu oraz reagowania na ewentualne pojawienie się skutków opóźnionych w czasie, a także możliwość oceny prawidłowości podjętych działań.

**2. Działania wobec uczestników zdarzenia (pokrzywdzony – sprawca – świadek, rodzice)**

* Działania wobec uczestników zdarzenia z zakresu naruszenia bezpieczeństwa w cyberprzestrzeni, powinny być dedykowane zarówno osobom pokrzywdzonym, sprawcom, jak i świadkom zdarzenia (z uwagi na zróżnicowany charakter incydentu). Niektóre formy dotyczyć mogą pracy wyłącznie z pokrzywdzonymi, inne wymagać będą zastosowania różnych działań wychowawczych i/lub dyscyplinarnych wobec sprawcy. Należy pamiętać, że podejmowane działania dotyczą w większości przypadków dzieci, więc stroną uczestniczącą jest także rodzic/opiekun, w takich przypadkach stosuje się odpowiednie przepisy prawa.
* Zasadnym jest, by podejmowane przez placówkę działania były zaplanowane, stopniowe, dostosowane do sytuacji oraz przebiegały w proponowanej kolejności:
* Rozmowa z uczestnikiem zdarzenia odpowiednia do charakteru zdarzenia oraz roli uczestnika (pokrzywdzony/sprawca/świadek). Nie należy stosować języka przekierowującego winę i odpowiedzialność za zdarzenie na osobę pokrzywdzoną.
* Powiadomienie rodziców/opiekunów uczestników zdarzenia oraz informowanie ich o podejmowanych działaniach i ewentualnych konsekwencjach regulaminowych oraz przedstawienie propozycji wsparcia.
* Powiadomienie policji/sądu rodzinnego w przypadku podejrzenia popełnienia czynu zabronionego[[8]](#footnote-8).
* Otoczenie wsparciem i opieką psychologiczno-pedagogiczną uczestników zdarzenia.

**3. Działania wobec instytucji/organizacji/służb pomocowych i współpracujących – policja, wymiar sprawiedliwości, służby społeczne.**

* Na instytucjach publicznych, takich jak szkoła i inne placówki oświatowe, spoczywa szczególny obowiązek współpracy z policją oraz sądem rodzinnym[[9]](#footnote-9). Szkoła i placówki oświatowe (obowiązek dyrektora placówki) są zobligowane do zawiadomienia policji lub sądu rodzinnego o popełnieniu przez dziecko czynu karalnego o którym dowiedziały się w związku ze swoją działalnością[[10]](#footnote-10). Ponadto spoczywa na nich obowiązek podjęcia niezbędnych czynności, aby nie dopuścić do zatarcia jego śladów oraz zabezpieczenia dowodów[[11]](#footnote-11)). Obowiązek powiadomienia policji przez dyrektora nie dotyczy czynów ściganych przez organy na wniosek pokrzywdzonego oraz z oskarżenia prywatnego, gdy w charakterze oskarżyciela występuje sam pokrzywdzony.
* W razie wystąpienia przez pokrzywdzonego ze skargą lub oskarżeniem, współpraca placówki oświatowej z policją oraz sądem rodzinnym może polegać w szczególności, na udzielaniu informacji i pomocy przy przeprowadzaniu czynności postępowania w szkole, przekazaniu dokumentów oraz udostępnieniu danych ucznia.
* Należy również pamiętać o społecznym obowiązku zawiadomienia o możliwości popełnienia przestępstwa Prokuratury lub Policji, który dotyczy każdego, kto dowiedział się o popełnieniu przestępstwa ściganego z urzędu[[12]](#footnote-12).

### III. Obowiązki koordynatora bezpieczeństwa w sieci

**Koordynator bezpieczeństwa w sieci** ma za zadanie zapewnić:

1. **Wytyczne w zakresie bezpiecznego nawigowania Internetu przez:**

* opracowanie regulaminu wewnętrznego dotyczącego bezpiecznego korzystania z sieci teleinformatycznych, w tym Internetu (dalej: zasady bezpiecznego korzystania z Internetu) do zapoznania w formie fizycznej, na stronie placówki albo jego akceptacja w momencie podłączenia się urządzenia do sieci;
* przedstawienie zasad bezpiecznego korzystania z Internetu dzieciom, personelowi i rodzicom oraz informowanie w przypadku aktualizacji regulaminu;
* opracowanie jednostronicowej informacji nt. zagrożeń i rozwiązań w zakresie zapewnienia bezpiecznych warunków korzystania z Internetu z użyciem urządzeń osobistych dla rodziców i opiekunów.

2. **Bezpieczne warunki korzystania z Internetu na urządzeniach placówki przez:**

* ustalenie zakresu blokowania dostępu do treści nielegalnych, szkodliwych i nieodpowiednich do wieku;
* instalację oraz regularną, przynajmniej raz w miesiącu, aktualizację oprogramowania blokującego dostęp do treści nielegalnych, szkodliwych i nieodpowiednich do wieku podopiecznych oraz aktualizację systemu operacyjnego urządzeń;
* ewaluację, co najmniej raz w roku, czy oprogramowanie zabezpieczające oraz blokujące i ustalony zakres jest adekwatny do potrzeb dzieci i zmieniającego się otoczenia Internetu;
* sprawdzenie, co najmniej raz w miesiącu, czy na urządzeniach placówki znajdują się treści nielegalne, szkodliwe i nieodpowiednie do wieku dzieci;
* cykliczne, przynajmniej raz w semestrze, spotkanie z dziećmi poświęcone zasadom bezpiecznego korzystania z Internetu.

### IV. Przegląd zasad korzystania z Internetu i urządzeń mobilnych

1. Stosowane oprogramowanie zabezpieczające oraz blokujące, w tym jego zakres powinien być poddawany ewaluacji przynajmniej raz w roku, albo gdy: zidentyfikowane zostanie nowe ryzyko lub zagrożenie, zmieni się sposób działalności placówki lub wprowadzona zostanie nowa technologia.

2. Przegląd standardów i polityk ochrony powinien uwzględniać m.in. standardy ochronymałoledzieci, zmieniające się otoczenie Internetu, potrzeby dzieci, zasady bezpiecznego korzystania z Internetu oraz ogólnie politykę placówki, zakres zadań osoby odpowiedzialnej za Internet, kompetencje cyfrowe personelu, podstawę programową oraz tematykę i charakter spotkań poświęconych bezpiecznemu korzystaniu z Internetu, aktualność i skuteczność wprowadzonych rozwiązań technologicznych, oraz opinie ze strony personelu, dzieci oraz rodziców w zakresie praktyczności stosowanych rozwiązań.

### V. Praktyczne informacje (Załącznik)

**Uwaga, to ważne!**

Ten dokument to materiał pomocniczy, jest jedynie podpowiedzią. Nie zawiera wszystkich zasad, a niektóre z nich mogą nie być przydatne w danej instytucji.

**Ogólne zalecenia**:

* Polityka Bezpieczeństwa:
  + - opracowanie polityki bezpieczeństwa informatycznego dostosowanej do potrzeb placówki;
  + - opracowanie zasad bezpiecznego korzystania z Internetu w sposób zrozumiały dla odbiorcy końcowego, odnoszący się do możliwości dostępu do sieci w sposób nielimitowany i nieograniczony przez dzieci oraz personel, w tym przez urządzenia osobiste (np. laptopy, tablety, smartwatche, urządzenia peryferyjne np. drukarki, skanery, kamery internetowe, monitory, wyświetlacze różnego rodzaju itp.) na terenie placówki; uwzględniający w zależności od potrzeb sytuację nauczania zdalnego.
  + - ustalając zakres blokowania dostępu do zasobów internetowych należy uwzględnić: wiek dzieci, specjalne potrzeby edukacyjne, niepełnosprawności oraz neuroróżnorodność, język ojczysty, celowość (co jest blokowane i dlaczego?; jak odnosi się to do potrzeb dzieci i aktualnej sytuacji?), kompetencje cyfrowe dzieci i personelu, świadomość ograniczeń (Internet nigdy nie będzie w 100% bezpieczny) oraz podejście oparte na reagowaniu i wyciąganiu wniosków z błędów, również przez wykorzystanie takich sytuacji jako okazji do ciągłego polepszania bezpieczeństwa i nauki dla dzieci.
* Audyt bezpieczeństwa:
  + - regularne przeglądy i audyty bezpieczeństwa systemów informatycznych.
* Współpraca z rodzicami:
  + - zapewnienie rodzicom dostępu i informowanie o narzędziach kontroli rodzicielskich np. podczas zebrań.
* Kanały skarg i monitorowanie:
  + - stworzenie kanałów wewnętrznych poprzez np. dedykowaną osobę, adres mailowy aby uczniowie i personel mogli zgłaszać podejrzane aktywności.

**I – poziom sieci wifi placówki**:

Zalecenia:

* Wdrożenie bezpiecznej konfiguracji sieci WiFi z silnymi hasłami
* Ustawienia zabezpieczające w routerze – korzystanie ze standardu WPA3 dla bezpiecznej komunikacji lub przy założeniu, że nie wszystkie urządzenia podłączane do sieci oferują obsługę najnowszych protokołów, ustawienie poziomu zabezpieczeń łączących dwa protokoły np. WPA2/WPA3 - wtedy każde z urządzeń wybiera sposób łączenia (nowsze – w sposób bardziej bezpieczny, a starsze – mniej)
* Zmiana domyślnego hasła administratora na routerze jeśli takie jest fabrycznie ustanowione
* Regularna aktualizacja oprogramowania routera (w panelu administracyjnym urządzenia). Możliwe jest również korzystanie z opcji automatycznej aktualizacji jeśli router posiada taką funkcję.
* Wyłączenie WPS (Wifi Protected Setup) – funkcji routerów bezprzewodowych która za pomocą przycisku na urządzeniu ułatwia łączenie nowych urządzeń z siecią bezprzewodową bez konieczności podawania hasła. Funkcja pozwala na chwilowe otwarcie sieci dla wszystkich.
* Wydzielić osobną sieć dla gości np. urządzeń, których placówka nie jest właścicielem. Sieć taka zapewni dostęp do Internetu, uniemożliwiając dostęp do innych urządzeń w sieci placówki.
* Wyłączenie opcji zdalnego dostępu do routera (dostępna w panelu administratora)
* Cykliczne sprawdzanie listy urządzeń podłączonych do głównej sieci wewnętrznej placówki. W przypadku nieznanego sprzętu – blokada.
* Konfiguracja DNS na routerze[[13]](#footnote-13). DNS-y mogą blokować domeny serwujące wybrane niepożądane treści np. materiały dla dorosłych[[14]](#footnote-14). Zmiana DNS na routerze spowoduje, że automatycznie wszystkie urządzenia podłączone w sieci zaczną korzystać ze wskazanych bezpiecznych domen. Zmiany dokonuje się w panelu administracyjnym routera.

**II – Poziom urządzeń**:

* Wdrożenie zasad korzystania z urządzeń i zabezpieczonych aplikacji.
* Aktualizacja oprogramowania urządzeń i ich monitorowanie pod kątem aktywności użytkownika.
* Wdrożenie rozwiązań antywirusowych.
* Ustawienia kontroli rodzicielskich na urządzeniach.
* Ograniczenie dostępu do urządzeń i zasobów tylko dla upoważnionych osób.
* Konfiguracja kont administratorów i użytkowników z ograniczonymi uprawnieniami na urządzeniach dostępnych dla uczniów.

**III – Poziom aplikacji edukacyjnych i użytkowych**:

* Ocena i wybór bezpiecznych aplikacji edukacyjnych i użytkowych (pobieranie tylko z pewnych źródeł, ze strony producentów aplikacji).
* Edukacja nauczycieli i uczniów w zakresie bezpiecznego korzystania z aplikacji.
* Monitorowanie i blokowanie podejrzanej aktywności w aplikacjach.

**IV – Poziom wyszukiwarek internetowych**:

* Filtry treści: rozszerzenie do przeglądarki, które chroni przed szkodliwymi treściami np. tryb SafeSearch w ustawieniach wyszukiwarki Google, konfiguracja ustawień przeglądarek pod kątem bezpieczeństwa i prywatności użytkowników. Ustawienia kontroli rodzicielskich w wyszukiwarkach.
* Edukacja uczniów w zakresie bezpiecznego wyszukiwania w zasobach internetowych.

**V – Poziom zarządzania zdarzeniami i reakcji na incydenty**

* Stworzenie planu zarządzania zdarzeniami.
* Szkolenie personelu w zakresie reakcji na incydenty – kogo powiadomić, w jaki sposób.

**VI – Podnoszenie świadomości i edukacja:**

* Wdrożenie programów edukacyjnych na temat bezpieczeństwa online np: Materiały do cyber lekcji: [Materiały do CYBER lekcji - Baza wiedzy - Portal Gov.pl (www.gov.pl)](https://www.gov.pl/web/baza-wiedzy/materialy-do-cyberlekcji)
* Współpraca z rodzicami w zakresie edukacji cyfrowej np.: aplikacja przeznaczona dla rodziców – mOchrona: aplikacja ochrony rodzicielskiej OSE, dostępna bezpłatnie na smartfony, tablety i komputery.[Aplikacja mOchrona – stworzona dla rodziców z myślą o dzieciach - Nie zagub dziecka w sieci - Portal Gov.pl (www.gov.pl)](https://www.gov.pl/web/niezagubdzieckawsieci/aplikacja-mochrona--stworzona-dla-rodzicow-z-mysla-o-dzieciach)
* Do kompetencji z zakresu efektywnego wykorzystywania mediów cyfrowych, które sprzyjają bezpiecznym relacjom między dziećmi zalicza się[[15]](#footnote-15): rozwijanie myślenia krytycznego, rozwijanie kompetencji miękkich w obszarze komunikacji oraz emocji, rozwijanie wiedzy nt. bieżących zagrożeń i trendów (np. Internet, media; społecznościowe, nowe technologie, zagrożenia prywatności itd.), rozwijanie zdolności do aktywnego poszukiwania pomocy, promowanie cyfrowej równowagi (digital wellbeing).
* Do minimalnych kompetencji osoby odpowiedzialnej za Internet zalicza się**:** kompetencje techniczne pozwalające na wprowadzenie zabezpieczeń informatycznych i zabezpieczeń różnego typu chroniących przed treściami nielegalnymi, nieodpowiednimi i szkodliwymi, zdolność rozumienia cyfrowej rzeczywistości – świadomość zagrożeń technicznych i społecznych, wiedza na temat metod i sposobu wykorzystywania mediów cyfrowych przez młodych ludzi, ciągłe szkolenie w zakresie reagowania na incydenty w ramach procedur danej placówki (np. reakcja na przemoc z wykorzystaniem technologii informacyjnej), kompetencje cyfrowe umożliwiające wykorzystywanie rozwiązań online w edukacji, prosta i efektywna komunikacja – dostosowanie języka i formy do odbiorcy.

**Dodatkowe wskazówki**

* Stosowanie oprogramowania antywirusowego na wszystkich urządzeniach.
* Regularne aktualizacje oprogramowania, aktualizacje systemów operacyjnych, aplikacji.
* Kontrola dostępu: ustawienia haseł i kont dla każdego użytkownika, ograniczenie dostępu tylko dla upoważnionych użytkowników (konta administracyjne oraz konta użytkowników na urządzeniach).
* Zabezpieczenia fizyczne: oznaczanie i rejestrowanie urządzeń oraz zamki i systemy antykradzieżowe.
* Kontrola rodzicielska: konfiguracja funkcji kontroli rodzicielskich na urządzeniach używanych przez dzieci, monitorowanie aktywności, odpowiednia konfiguracja przeglądarek, audyty systemów i historii przeglądania i pobierania.
* Szyfrowanie danych: Szyfrowanie wrażliwych danych przechowywanych na urządzeniach np. danych osobowych o uczniach, rodzicach, pracownikach itp.
* Zabezpieczanie urządzeń peryferyjnych w tym IoT np. poprzez zmianę domyślnych haseł administracyjnych, ograniczenie dostępu do pomieszczeń w których się znajdują, przydzielanie uprawnień użytkownikom uprawnionych do korzystania.
* Placówka nie może brać i nie bierze odpowiedzialności za poziom zabezpieczeń urządzeń osobistych. Pozostaje to w indywidualnej gestii użytkownika. Placówka w tym zakresie może promować dobre praktyki i edukować poprzez nauczycieli, rodziców i zaproszonych gości. Urządzenia prywatne/osobiste będące w posiadaniu użytkowników (uczniów, nauczycieli) powinny podłączać się do wydzielonej sieci dla gości (którą można skonfigurować na routerze).

**O czym należy pamiętać (z poziomu technicznego) dokonując wyboru konkretnego oprogramowania, tak aby wszystkie elementy występujące w środowisku szkolnym były możliwie, jak najlepiej zabezpieczone?**

* Oprogramowanie powinno pochodzić od sprawdzonego dostawcy, godnego zaufania, z solidnymi praktykami bezpieczeństwa, certyfikowanego (warto przeanalizować historię firmy, zapoznać się z recenzjami, opiniami innych podmiotów, czy doświadczeniami użytkowników).
* Oprogramowanie powinno oferować mechanizmy szyfrowania danych, szczególnie jeśli przetwarza ono wrażliwe informacje o personelu czy uczniach.
* Należy wybrać oprogramowanie, które jest regularnie aktualizowane przez dostawcę (poprawki bezpieczeństwa).
* Zależnie od przeznaczenia oprogramowanie może umożliwiać zarządzanie dostępem lub kontrolę, kto ma dostęp do określonych funkcji i danych.
* Należy sprawdzić, w miarę możliwości, czy oprogramowanie posiada certyfikaty bezpieczeństwa lub jest zgodne z międzynarodowymi standardami bezpieczeństwa.
* Należy zweryfikować, czy istnieje możliwość skontaktowania się z producentem oprogramowania w przypadku wystąpienia błędów. Warto sprawdzić, czy dostawca oferuje mechanizmy zgłaszania incydentów bezpieczeństwa i jak szybko reaguje na potencjalne problemy.
* Warto zapoznać się z polityką prywatności dostawcy oprogramowania. Upewnić się, że jest ona zgodna z obowiązującymi przepisami dotyczącymi ochrony prywatności np. RODO.
* Jeśli oprogramowanie będzie integrowane z innymi systemami w placówce, należy upewnić się, że integracje są bezpieczne i zgodne z obowiązującymi standardami.
* Warto zweryfikować, czy oprogramowanie ma mechanizmy regularnego backupu danych (wykonywania kopii zapasowych), aby zminimalizować ryzyko utraty informacji.
* W przypadku wdrożenia nowego oprogramowania, jeśli będzie ono przeznaczone do użytkowania przez pracowników/uczniów placówki, należy zorganizować szkolenia dotyczące korzystania z oprogramowania w sposób bezpieczny. To kluczowe, aby uniknąć potencjalnych zagrożeń wynikających z braku wiedzy.
* Ważny jest również element dotyczący bezpieczeństwa poczty e-mail i phishingu w sieci, zwłaszcza w aspekcie korzystania przez pracowników z poczty na urządzeniach służbowych i ryzyka phishingu oraz zagrożeń dla sieci wewnętrznej placówki wynikających z tego typu ataków. Także w aspekcie otrzymywania przez uczniów wszelkiego rodzaju SPAM-u, ofert, treści niewłaściwych – co z tym zrobić, jak się zachować.
* **Bezpieczeństwo to proces ciągły, a wybór bezpiecznego oprogramowania to jedynie jeden z elementów całego systemu bezpieczeństwa w placówce**.

1. Art. 202 § 3, § 4, § 4a, § 4b Kodeksu karnego [↑](#footnote-ref-1)
2. Art. 202 § 3 Kodeksu karnego [↑](#footnote-ref-2)
3. Art. 256 Kodeksu karnego [↑](#footnote-ref-3)
4. Art. 200b Kodeksu karnego [↑](#footnote-ref-4)
5. Art. 191a Kodeksu karnego [↑](#footnote-ref-5)
6. Art. 200 § 3, 4 Kodeksu karnego [↑](#footnote-ref-6)
7. Art. 200a Kodeksu karnego [↑](#footnote-ref-7)
8. Zgłoszenie na policję, <https://dyzurnet.pl/uploads/2023/12/Ulotka_zglosc-na-policje.pdf>. [↑](#footnote-ref-8)
9. Art.  304 § 2 Kodeksu postępowania karnego. [↑](#footnote-ref-9)
10. Art. 4 § 2, ustawa z dnia 9 czerwca 2022 r. o wspieraniu i resocjalizacji nieletnich (Dz. U. 2022 poz. 170). [↑](#footnote-ref-10)
11. Art. 4 § 3, ustawa z dnia 9 czerwca 2022 r. o wspieraniu i resocjalizacji nieletnich (Dz. U. 2022 poz. 170). [↑](#footnote-ref-11)
12. art. 304 § 1 k.p.k. [↑](#footnote-ref-12)
13. W przypadku korzystanie z OSE nie jest to konieczne. [↑](#footnote-ref-13)
14. Np. Cloudflare w wersji „Family” które oprócz stron z pornografią blokują także strony ze złośliwym oprogramowaniem: 1.1.1.3 oraz 1.0.0.3. [↑](#footnote-ref-14)
15. Przykładowe materiały np. <https://edukacja.fdds.pl/course/view.php?id=380>. [↑](#footnote-ref-15)