PROCEDURY REAGOWANIA W PRZYPADKU WYSTĄPIENIA W SZKOLE ZAGROŻEŃ BEZPIECZEŃSTWA CYFROWEGO

Podejmowane w placówce obligatoryjne działania interwencyjne, będące następstwem wystąpienia zagrożenia, dzielą się na 3 grupy:

1) działania wobec aktu/zdarzenia - opis przypadku, ustalenie okoliczności zdarzenia, zabezpieczenie dowodów oraz monitoring po interwencyjny.

2) działania wobec uczestników zdarzenia (ofiara - sprawca - świadek, rodzice).

3) działania wobec instytucji/organizacji/służb pomocowych i współpracujących – Policji, wymiaru sprawiedliwości, służb społecznych.

Działania wobec zdarzenia polegają przede wszystkim na zachowaniu (nie usuwaniu) dokumentacji cyfrowej: wiadomości sms, e-maili, nagrań z poczty głosowej telefonu, komentarzy w serwisie społecznościowym, zapisów w blogu i plików filmów wideo.

O ile to możliwe, należy także zarchiwizować treść rozmów w komunikatorach oraz linki (konkretne adresy URL) oraz danych o potencjalnym sprawcy.

Każde zdarzenie wymaga udokumentowania w stosownym protokole.

Działania na rzecz uczestników zdarzenia to aktywności podejmowane wobec ofiar (osób poszkodowanych), sprawców i świadków zdarzenia oraz ich rodziców.

Procedura reakcji w sytuacji zagrożenia obejmuje następujące etapy:

1. Rozmowa uczestnika zdarzenia z dyrektorem szkoły.
2. Powiadomienie rodziców/ opiekunów poszkodowanego dziecka.
3. Działania wychowawcze i wyciagnięcie konsekwencji wobec sprawcy.
4. Powiadomienie Policji/ sądu rodzinnego w przypadku naruszenia prawa.
5. Udzielenie uczestnikom zdarzenia wsparcia psychologicznego.

Działania szkoły adresowane do instytucji i organizacji zewnętrznych są niezbędne w przypadku naruszenia przepisów prawa przez uczniów lub osoby spoza szkoły. Pośród nich należy wyróżnić szczególnie współpracę z: policją i sądami rodzinnymi, służbami społecznymi i placówkami specjalistycznymi oraz dostawcami usług internetowych i operatorami telekomunikacyjnymi.

Sprawców wszystkich rodzajów zagrożeń bezpieczeństwa cyfrowego w szkole należy objąć , co najmniej, poniższymi działaniami:

1) Sprawca musi otrzymać od przedstawicieli szkoły komunikat o braku akceptacji dla działań , jakich dokonał.
2) W trakcie takiej rozmowy uczeń powinien poznać możliwe skutki swojego postępowania, a także konsekwencje, jakie mogą zostać wobec niego wyciągnięte (np. wynikające z statutu).
3) W trakcie rozmowy sprawca powinien zostać wezwany do zaprzestania podejmowania podobnych działań w przyszłości, w tym usunięcia skutków swoich działań (np. publikacji w portalu społecznościowym).
4) Sprawcę należy objąć odpowiednią pomocą psychologiczną - pedagogiczną w celu uświadomienia mu konsekwencji jego zachowania, skłonienia go do zmiany postawy

i postępowania.

5) Jeśli sprawców jest więcej, to z każdym z nich należy rozmawiać osobno.
6) Należy zadbać o to, żeby osoba reprezentująca szkołę (psycholog, pedagog, wychowawca) ograniczała się do podjęcia interwencji, a nie wymierzała karę. Decyzję o tym, jaką karę wymierzyć sprawcy, powinna podejmować rada pedagogiczna (po poznaniu wszystkich okoliczności zdarzenia), a przekazywać dyrektor szkoły.
   Ważne jest oddzielenie osoby pedagoga, nawiązującego relację z uczniem, od organu wymierzającego karę.
7) Celem sankcji wobec sprawcy jest przede wszystkim: zatrzymanie jego działań i zapewnienie poczucia bezpieczeństwa ofierze, zmiana postawy sprawcy, zasygnalizowanie społeczności szkolnej braku tolerancji wobec negatywnych działań tego typu i udowodnienie, że szkoła jest w stanie skutecznie zareagować.
8) Podejmując decyzję o sankcjach, należy wziąć pod uwagę:
   - <u>rozmiar i rangę szkody</u> – np. czy w przypadku cyberprzemocy materiał został upubliczniony w sposób pozwalający na dotarcie do niego wielu osobom (określa to rozmiar upokorzenia, jakiego doznaje ofiara), czy trudno jest wycofać materiał z sieci, itp.
   - <u>czas trwania prześladowania</u> – czy było to długotrwałe działanie, czy pojedynczy incydent
   - <u>świadomość popełnianego czynu</u> – czy działanie było zaplanowane, a sprawca był świadomy, że postąpił nagannie, np. czy wie, że wyrządza krzywdę koledze, jak wiele wysiłku włożył w ukrycie swojej tożsamości, itp.
   - <u>motywację sprawcy</u> – należy sprawdzić , czy działanie sprawcy nie jest działaniem odwetowym w odpowiedzi na uprzednie doświadczenia sprawcy.

9) Aktywność wobec sprawcy powinna także obejmować rozmowę z jego rodzicami lub opiekunami prawnymi – powinni oni zostać poinformowani o zdarzeniu, zapoznani z materiałami oraz decyzją na temat dalszego postępowania ze sprawcą (np. na temat sankcji).
   Warto, aby rodzice współpracowali ze szkołą w zakresie rozwiązywania sytuacji kryzysowej, aby stali się jej sojusznikami, a nie przeciwnikami. Rodzice sprawcy powinni również zostać poinformowani, że rodzice ofiary mają prawo zgłosić sprawę na Policję.

10) Jeśli sprawca pochodzi spoza szkoły, należy zapewnić bezpieczeństwo ofierze i poinformować ją (jej rodziców) o przysługujących jej prawach, (np. zgłoszenie popełnienie przestępstwa na Policję). Jeśli sprawca jest z innej szkoły, należy rozważyć nawiązanie współpracy między placówkami i wspólne rozwiązanie kryzysowej sytuacji.

Szczegółowe procedury na wypadek wystąpienia zagrożeń bezpieczeństwa cyfrowego.

1. Dostęp do treści szkodliwych, niepożądanych, nielegalnych - procedura reagowania

Podstawy prawne uruchomienia procedury	Kodeks Karny, Statut szkoły
Rodzaj zagrożenia objętego procedurą	Zagrożenie łatwym dostępem do treści szkodliwych, niedozwolonych, nielegalnych i niebezpiecznych dla zdrowia (pornografia, treści obrazujące przemoc i promujące działania szkodliwe dla zdrowia i życia dzieci, popularyzujące ideologię faszystowską i działalność niezgodną z prawem, nawoływanie do samookaleczeń i samobójstw, korzystania z narkotyków; niebezpieczeństwo werbunku dzieci i młodzieży do organizacji nielegalnych i terrorystycznych)
Telefony/kontakty alarmowe krajowe	Zgłaszanie nielegalnych treści: dyzurnet@dyzurnet.pl, tel. 801 615 005, Policja 997
SPOSÓB POSTĘPOWANIA W PRZYPADKU WYSTĄPIENIA ZAGROŻENIA	
Opis okoliczności, analiza, zabezpieczenie dowodów	Reakcja szkoły w przypadku pozyskania wiedzy o wystąpieniu zagrożenia będzie zależna od tego, czy: (1) treści te można bezpośrednio powiązać z uczniami danej szkoły, czy też (2) treści nielegalne lub szkodliwe nie mają związku z uczniami danej szkoły, lecz wymagają kontaktu szkoły z odpowiednimi służbami. W pierwszej kolejności należy zabezpieczyć dowody w formie elektronicznej (pliki z treściami niedozwolonymi, zapisy rozmów w komunikatorach, e-maile, zrzuty ekranu), znalezione w Internecie lub w komputerze dziecka. Zabezpieczenie dowodów jest zadaniem rodziców lub opiekunów prawnych dziecka, w czynnościach tych może wspomagać ich przedstawiciel szkoły posiadający odpowiednie kompetencje techniczne. W przypadku sytuacji (1) rozwiązanie leży po stronie szkoły, zaś (2) należy rozważyć zgłoszenie incydentu na Policję oraz zgłosić go do serwisu Dyżurnet (dyzurnet.pl).
Identyfikacja sprawcy (-ów)	W identyfikacji sprawców kluczowe znaczenie odgrywać będą zgromadzone dowody. W procesie udostępniania nielegalnych i szkodliwych treści małoletnim występują na ogół: twórca treści (np. pornografii) oraz osoby, która udostępniły je dziecku. Często osobami tymi są rówieśnicy – uczniowie tej samej szkoły czy klasy, dzieci sąsiadów. Konieczne jest poinformowanie wszystkich rodziców lub opiekunów dzieci uczestniczących w zdarzeniu o sytuacji i roli ich dzieci.
Działania wobec sprawców zdarzenia ze szkoły/ spoza szkoły	W przypadku udostępniania (szerowania, dzielenia się) treści opisanych wcześniej jako szkodliwych/ niedozwolonych/nielegalnych i niebezpiecznych dla zdrowia przez ucznia należy przeprowadzić z nim rozmowę na temat jego postępowania i w jej trakcie uzmysłowić mu szkodliwość prowadzonych przez niego działania. Działania szkoły powinny koncentrować się jednak na aktywnościach wychowawczych. W przypadku upowszechniania przez sprawców treści nielegalnych (np. pornografii dziecięcej) należy złożyć zawiadomienie o zdarzeniu na Policję.
Aktywności wobec ofiar zdarzenia	Dzieci - ofiary i świadków zdarzenia – należy od pierwszego etapu interwencji - otoczyć opieką psychologiczno-pedagogiczną. Rozmowa z dzieckiem powinna się odbywać w warunkach jego komfortu psychicznego, z poszanowaniem poufności i podmiotowości ucznia ze

	względu na fakt, iż kontakt z treściami nielegalnymi może mieć bardzo szkodliwy wpływ na jego psychikę. W jej trakcie należy ustalić okoliczności uzyskania przez ofiarę dostępu do ww. treści. Należy koniecznie powiadomić ich rodziców lub opiekunów prawnych o zdarzeniu i uzgodnić z nimi podejmowane działania i formy wsparcia dziecka. Działania szkoły w takich przypadkach powinna cechować poufność i empatia w kontaktach z wszystkimi uczestnikami zdarzenia oraz udzielającymi wsparcia. W przypadku kontaktu dziecka z treściami szkodliwymi należy dokładnie zbadać sposób, w jaki nastąpił kontakt dziecka z nimi. Poszukiwanie przez dziecko tego typu treści w sieci lub podsuwanie ich dziecku przez innych może być oznaką niepokojących incydentów ze świata rzeczywistego. Np. kontakty z osobami handlującymi narkotykami czy proces rekrutacji do sekty lub innej niebezpiecznej grupy.
Współpraca z Policją i sądami rodzinnym	W przypadku naruszenia prawa, np. rozpowszechniania materiałów pornograficznych z udziałem nieletniego lub prób uwiedzenia małoletniego w wieku do 15 lat przez osobę dorosłą, należy – w porozumieniu z rodzicami dziecka - niezwłocznie powiadomić Policję
Współpraca ze służbami i placówkami specjalistycznymi	Kontakt z treściami szkodliwymi lub niebezpiecznymi może wywołać potrzebę skorzystania przez ofiarę ze specjalistycznej opieki psychologicznej. Decyzja o takim kontakcie i skierowaniu na terapię musi zostać podjęta w porozumieniu z rodzicami/opiekunami prawnymi dziecka.

2. Cyberprzemoc – procedura reagowania

Podstawy prawne uruchomienia procedury	Kodeks Karny, Statut szkoły
Rodzaj zagrożenia objętego procedurą	Cyberprzemoc – przemoc z użyciem technologii informacyjnych i komunikacyjnych, głównie Internetu oraz telefonów komórkowych. Podstawowe formy zjawiska to nękanie, straszenie, szantażowanie z użyciem sieci, publikowanie lub rozsyłanie ośmieszających, kompromitujących informacji, zdjęć , filmów z użyciem sieci oraz podszywanie się w sieci pod kogoś wbrew jego woli. Do działań określanych mianem cyberprzemocy wykorzystywane są głównie: poczta elektroniczna, czaty, komunikatory, strony internetowe, blogi, serwisy społecznościowe, grupy dyskusyjne, serwisy SMS i MMS.
Telefony/kontakty alarmowe krajowe	Telefon Zaufania dla Dzieci i Młodzieży - 116 111 Telefon dla Rodziców i Nauczycieli w sprawie Bezpieczeństwa Dzieci – 800 100 100, dyzurnet@dyzurnet.pl
SPOSÓB POSTĘPOWANIA W PRZYPADKU WYSTĄPIENIA ZAGROŻENIA	
Przyjęcie zgłoszenia i ustalenie okoliczności zdarzenia	Przypadek cyberprzemocy może zostać ujawniony przez ofiarę, świadka (np. innego ucznia, nauczyciela, rodzica) lub osobę bliską ofierze (np. rodzice, rodzeństwo, przyjaciele).

	W każdym przypadku należy ze spokojem wysłuchać osoby zgłaszającej i okazać jej wsparcie. Podziękować za zaufanie i zgłoszenie tej sprawy. Jeśli zgłaszającym jest ofiara cyberprzemocy, podejmując działania, przede wszystkim należy okazać wsparcie, z zachowaniem jej podmiotowości i poszanowaniem jej uczuć . Potwierdzić , że ujawnienie przemocy jest dobrą decyzją. Taką rozmowę należy przeprowadzić w miejscu bezpiecznym, zapewniającym ofierze intymność . Nie należy podejmować kroków, które mogłyby prowadzić do powtórnej wiktymizacji czy wzbudzić podejrzenia sprawcy (np. wywoływać ucznia z lekcji do dyrekcji). Jeśli osobą zgłaszającą nie jest ofiara, na początku prosimy o opis sytuacji, także z zachowaniem podmiotowości i poszanowaniem uczuć osoby zgłaszającej (np. strach przed byciem kapusiem, obawa o własne bezpieczeństwo). W każdej sytuacji w trakcie ustalania okoliczności trzeba ustalić charakter zdarzenia (rozmiar i rangę szkody, jednorazowość /powtarzalność). Realizując procedurę należy unikać działań , które mogłyby wtórnie stygmatyzować ofiarę lub sprawcę, np.: wywoływanie uczniów z lekcji, konfrontowanie ofiary i sprawcy, niewspółmierna kara, wytykanie palcami, etc. Trzeba dokonać oceny, czy zdarzenie wyczerpuje znamiona cyberprzemocy, czy jest np. niezbyt udanym żartem (wtedy trzeba podjąć działania profilaktyczne mające na celu niedopuszczenie do eskalacji tego typu zachowań w stronę cyberprzemocy).
Opis okoliczności, analiza, zabezpieczenie dowodów	Należy zabezpieczyć wszystkie dowody związane z aktem cyberprzemocy (np. zrobić kopię materiałów, zanotować datę i czas otrzymania materiałów, dane nadawcy, adresy stron www, historię połączeń , etc.). W trakcie zbierania materiałów należy zadbać o bezpieczeństwo osób zaangażowanych w problem.
Identyfikacja sprawcy(-ów)	Identyfikacja sprawcy(o w) często jest możliwa dzięki zebranym materiałom – wynikom rozmów z osobą zgłaszającą, z ofiarą, analizie zebranych materiałów. Ofiara często domyśla się, kto stosuje wobec niego cyberprzemoc. Jeśli ustalenie sprawcy nie jest możliwe, a w ocenie kadry pedagogicznej jest to konieczne, należy skontaktować się z Policją. Bezwzględnie należy zgłosić rozpowszechnianie nagich zdjęć osób poniżej 18 roku życia (art. 202 par. 3 KK)
Aktywności wobec sprawców zdarzenia ze szkoły/ spoza szkoły	Gdy sprawca cyberprzemocy jest znany i jest on uczniem szkoły, pedagog szkolny powinien

	przeprowadzić z nim rozmowę o jego zachowaniu. Rozmowa taka ma służyć ustaleniu okoliczności zdarzenia, jego wspólnej analizie (w tym np. przyjrzeniu się przyczynom), a także próbie rozwiązania sytuacji konfliktowej (w tym sposobów zadośćuczynienia ofiarom cyberprzemocy). Cyberprzemoc powinna podlegać sankcjom określonym w wewnętrznych przepisach szkoły (m. in. w statucie).
Aktywności wobec ofiar zdarzenia	W pierwszej kolejności należy udzielić wsparcia ofierze. Musi się ona czuć bezpieczna i otoczona opieką przez dorosłych. Na poczucie bezpieczeństwa dziecka wpływa fakt, że wie ono, iż szkoła podejmuje kroki w celu rozwiązania problemu. Podczas rozmowy z uczniem – ofiarą cyberprzemocy – należy zapewnić go, że nie jest winny zaistniałej sytuacji oraz że nikt nie ma prawa zachowywać się w ten sposób wobec niego, a także podkreślić , że dobrze zrobił ,ujawniając sytuację. Należy okazać zrozumienie dla jego uczuć , w tym trudności z ujawnieniem okoliczności wydarzenia, strachu, wstydu. Trzeba podkreślić , że szkoła nie toleruje przemocy i że zostaną podjęte odpowiednie procedury interwencyjne. Należy poinformować ucznia o krokach, jakie może podjąć szkoła i sposobach, w jaki może zapewnić mu bezpieczeństwo. Należy pomóc ofierze (rodzicom ofiary) w zabezpieczeniu dowodów (to może być dla niej zadanie trudne zarówno ze względów technicznych, jak i emocjonalnych), zerwaniu kontaktu ze sprawcą, zadbaniu o podstawowe zasady bezpieczeństwa on-line (np. nieudostępnianie swoich danych kontaktowych, kształtowanie swojego wizerunku, etc). Pomoc ofierze nie może kończyć się w momencie zakończenia procedury. Warto monitorować sytuację, „czuwać ” nad jej bezpieczeństwem, np. zwracać uwagę, czy nie są podejmowane wobec niej dalsze działania przemocowe, obserwować, jak sobie radzi w grupie po ujawnionym incydencie cyberprzemocy. W działania wobec ofiary należy także włączyć rodziców/opiekunów ofiary – trzeba na bieżąco ich informować o sytuacji, pamiętając przy tym o podmiotowym traktowaniu dziecka – mówiąc mu o tym i starając się uzyskać jego akceptację dla udziału rodziców. Jeśli dziecko nie wyraża zgody, należy omówić z nim jego obawy, a jeśli to nie pomaga powołać się na obowiązujące nas zasady i przekazać informację rodzicom. W trakcie rozmowy z dzieckiem i/lub jego

	rodzicami/opiekunami, jeśli jest to wskazane, można zaproponować pomoc specjalisty (np. psycholog szkolny, poradnia psychologiczno-pedagogiczna) oraz przekazać informację o możliwości zgłoszenia sprawy Policji.
Aktywności wobec świadków	Należy zadbać o bezpieczeństwo świadków zdarzenia, zwłaszcza, jeśli byli oni osobami ujawniającymi cyberprzemoc. W trakcie rozmowy ze świadkami należy okazać zrozumienie i empatię dla ich uczuć– obawy przed przypięciem łatki „donosiciela", strachu przed staniem się kolejną ofiarą sprawcy, itp.
Współpraca z Policją i sądami rodzinnymi	Samo wystąpienie zjawiska cyberprzemocy nie jest jednoznaczne z koniecznością zaangażowania Policji i sądu rodzinnego – procedura powinna umożliwiać rozwiązanie sytuacji problemowej na poziomie pracy wychowawczej szkoły. Szkoła powinna powiadomić odpowiednie służby (np. sąd rodzinny), gdy wykorzysta wszystkie dostępne jej środki wychowawcze (rozmowa z rodzicami, konsekwencje z statutu i/lub regulaminu wobec ucznia) i interwencje pedagogiczne, a ich zastosowanie nie przynosi pożądanych rezultatów (np. nie ma zmian postawy ucznia). Kontaktu z Policją wymagają wszelkie sytuacje, w których zostało naruszone prawo (np. groźby karalne, świadome publikowanie nielegalnych treści, rozpowszechnianie nagich zdjęć z udziałem małoletnich). Za zgłoszenie odpowiada dyrektor szkoły.
Współpraca z dostawcami Internetu i operatorami telekomunikacyjnymi	Kontakt z dostawcą usługi może być wskazany w celu usunięcia z sieci kompromitujących lub krzywdzących materiałów. Do podjęcia takiego działania zobowiązuje administratora serwisu art. 14 Ustawy z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną.

3. Naruszenia prywatności dotyczące nieodpowiedniego lub niezgodnego z prawem wykorzystania danych osobowych lub wizerunku dziecka i pracownika szkoły - procedura reagowania

Podstawy prawne uruchomienia procedury	Kodeks Karny (art. 190a par. 2)
Rodzaj zagrożenia objętego procedurą	Zagrożenie to polega na naruszeniu prywatności dziecka lub pracownika szkoły poprzez nieodpowiednie lub niezgodne z prawem wykorzystanie danych osobowych lub wizerunku dziecka i pracownika szkoły. Należy zwrócić uwagę, iż podszywanie się pod inną osobę, wykorzystywanie jej wizerunku lub

	danych osobowych w celu wyrządzenia jej szkody osobistej lub majątkowej jest w świetle polskiego prawa przestępstwem. Najczęstszymi formami wyłudzenia lub kradzieży danych jest przejęcie profilu na portalu społecznościowym w celu dyskredytacji lub naruszenia dobrego wizerunku ofiary (np. publikacja zdjęć intymnych bądź montowanych), szantażu (w celu uzyskania korzyści finansowych w zamian za niepublikowanie zdjęć bądź treści naruszających dobry wizerunek ofiary), dokonania zakupów i innych transakcji finansowych (np. w sklepach internetowych na koszt ofiary) lub uzyskania korzyści (np. usługi premium SMS). Często naruszenia prywatności łączy się z cyberprzemocą.
SPOSÓB POSTĘPOWANIA W PRZYPADKU WYSTĄPIENIA ZAGROŻENIA	
Przyjęcie zgłoszenia i ustalenie okoliczności zdarzenia	Gdy sprawcą jest uczeń - kolega ofiary ze szkoły czy klasy, uczniowie lub rodzice winni skontaktować się z dyrektorem szkoły, wychowawcą lub Szkolnym Mentorem Bezpieczeństwa Cyfrowego. W przypadku, gdy do naruszenia prywatności poprzez kradzież, wyłudzenie danych osobowych wykorzystanie wizerunku dziecka dochodzi ze strony dorosłych osób trzecich, rodzice winni skontaktować się bezpośrednio z Policją i powiadomić o tym szkołę (zgodnie z Kodeksem Karnym ściganie następuje tu na wniosek pokrzywdzonego). Istotne dla ścigania sprawcy będzie uzyskanie dowodów, że sprawca zmierzał do wyrządzenia ofierze szkody majątkowej lub osobistej. Samo podszywanie się pod ofiarę nie jest karalne.
Opis okoliczności, analiza, zabezpieczenie dowodów	W pierwszej kolejności należy zabezpieczyć dowody nieodpowiedniego lub niezgodnego z prawem działania - w formie elektronicznej (e-mail, zrzut ekranu, konwersacja w komunikatorze lub sms). Równolegle należy dokonać zmian tych danych identyfikujących, które zależą od ofiary, tj. haseł i loginów lub kodów dostępu do platform i portali internetowych, tak aby uniemożliwić kontynuację procederu naruszania prywatności - w działaniu tym ucznia i/lub jego rodzica/opiekuna prawnego powinien wspierać Szkolny Mentor Bezpieczeństwa Cyfrowego. Jeśli wykradzione dane zostały wykorzystane w celu naruszenia dobrego wizerunku ofiary, bądź w innych celach niezgodnych z prawem należy dążyć do wyjaśnienia tych działań i usunięcia ich skutków, także tych widocznych w Internecie. Likwidacja stron internetowych czy profili w

	portalach społecznościowych, która wymagać będzie interwencji w zebrane dowody musi odbywać się za zgodą Policji (o ile została powiadomiona). Szczególnej uwagi wymagają incydenty kradzieży tożsamości w celu posłużenia się nią np. podczas zakupu towarów online lub dokonania transakcji finansowych. W tym przypadku należy skontaktować się ze sklepem lub pożyczkodawcą i wyjaśnić charakter zdarzenia.
Identyfikacja sprawcy(-ów)	W przypadku, gdy dowody jasno wskazują na konkretnego sprawcę oraz na spełnianie przesłanki, iż sprawca zmierzał do wyrządzenia ofierze szkody majątkowej lub osobistej należy je zabezpieczyć i przekazać Policji. W przypadku, gdy trudno to ustalić, identyfikacji dokonać winna Policja. W przypadku znanego sprawcy, który jednak nie działał z powyższych pobudek, szkoła powinna dążyć do rozwiązania problemu w ramach działań wychowawczo – edukacyjnych uzgodnionych rodzicami.
Aktywności wobec sprawców zdarzenia ze szkoły/ spoza szkoły	Gdy sprawcą incydentu jest uczeń szkoły, należy wobec niego – w porozumieniu z rodzicami – podjąć działania wychowawcze, zmierzające do uświadomienia nieodpowiedniego i nielegalnego charakteru czynów, jakich dokonał. Jednym z elementów takich działań powinny być przeprosiny złożone osobie poszkodowanej. Celem takich działań winno być nie tylko nabycie odpowiedniej wiedzy przez ucznia na temat wagi poszanowania prywatności w codziennym życiu, ale trwała zmiana jego postawy na akceptującą szacunek dla wizerunku i prywatności. Działania takie szkoła winna podjąć niezależnie od powiadomienia Policji/ sądu rodzinnego. Dyrekcja szkoły winna podjąć decyzje w sprawie powiadomienia o incydencie Policji, biorąc pod uwagę wiek sprawcy, jego dotychczasowe zachowanie, postawę po odkryciu incydentu oraz opinie wychowawcy i pedagoga. Przed podjęciem decyzji o zgłoszeniu incydentu na Policję należy rozważyć, czy istnieją dowody, iż uczeń - sprawca zmierzał do wyrządzenia ofierze szkody majątkowej lub osobistej. W takim przypadku dobrym rozwiązaniem jest uzyskanie interpretacji prawnej adwokata lub radcy prawnego.
Aktywności wobec ofiar zdarzenia	Ofiary incydentów należy otoczyć – w porozumieniu z rodzicami/opiekunami prawnymi - opieką pedagogiczno-

	psychologiczną i powiadomić o działaniach podjętych w celu usunięcia skutków działania sprawcy (np. usunięcie z Internetu intymnych zdjęć ofiary, zablokowanie dostępu do konta w portalu społecznościowym). Jeśli kradzież tożsamości, bądź naruszenie dobrego wizerunku ofiary jest znane tylko jej i rodzicom, szkoła winna zapewnić poufność działań, tak aby informacje narażające ofiarę na naruszenie wizerunku nie były rozpowszechniane.
Aktywności wobec świadków	Gdy kradzież tożsamości, bądź naruszenie dobrego wizerunku ofiary jest znane szerszemu gronu uczniów szkoły, należy podjąć wobec nich działania wychowawcze, zwracające uwagę na negatywną ocenę naruszania wizerunku ucznia – koleżanki lub kolegi oraz ryzyko penalizacji.
Współpraca z Policją i sądami rodzinnymi	Gdy naruszenie prywatności, czy wyłudzenie lub kradzież tożsamości skutkują wyrządzeniem ofierze szkody majątkowej lub osobistej, rodzice dzieci winni o nim powiadomić Policję.
Współpraca ze służbami i placówkami specjalistycznymi	W przypadku konieczności podejmowania dalszych działań pomocowych wobec ofiary, można skierować ucznia, za zgodą i we współpracy z rodzicami, do placówki specjalistycznej, np. terapeutycznej.

4.Zagrożenia dla zdrowia dzieci w związku z nadmiernym korzystaniem z Internetu – procedura reagowania

Podstawy prawne uruchomienia procedury	Ustawa z dnia 14 grudnia 2016 r. - Prawo oświatowe
Rodzaj zagrożenia objętego procedurą	Infoholizm (siecioholizm) – nadmierne, obejmujące niekiedy niemal całą dobę korzystanie z zasobów Internetu i gier komputerowych (najczęściej sieciowych) i portali społecznościowych przez dzieci. Jego negatywne efekty polegają na pogarszaniu się stanu zdrowia fizycznego (np. choroby oczu, padaczka ekranowa, choroby kręgosłupa) i psychicznego (irytacja, rozdrażnienie, spadek sprawności psychofizycznej, a nawet depresja), zaniedbywaniu codziennych czynności, oraz osłabianiu relacji rodzinnych i społecznych.
SPOSÓB POSTĘPOWANIA W PRZYPADKU WYSTĄPIENIA ZAGROŻENIA	
Przyjęcie zgłoszenia i ustalenie okoliczności zdarzenia	Infoholizm stwierdza najczęściej rodzic lub opiekun prawny dziecka. W przypadku konieczności podejmowania dalszych działań pomocowych można skierować ucznia, za zgodą i we współpracy z rodzicami, do placówki specjalistycznej, np. terapeutycznej. Kluczowe są tutaj pozostałe objawy wskazane wyżej.

	Nauczyciele w szkole także powinni zainteresować się przypadkami dzieci nieangażujących się w życie klasy, a poświęcającymi wolne chwile na kontakt online lub przychodzącymi do szkoły po nieprzespanej nocy. Rzadziej zgłoszeń można się spodziewać od rówieśników dziecka nadmiernie korzystającego z sieci.
Opis okoliczności, analiza, zabezpieczenie dowodów	Reakcja szkoły powinna polegać w pierwszych krokach na ustaleniu skutków zdrowotnych i psychicznych, jakie nadmierne korzystanie z zasobów Internetu wywołało u dziecka (np. gorsze oceny w nauce, niedosypianie, niedojadanie, rezygnacja z dawnych zainteresowań, załamanie się relacji z rodziną czy rówieśnikami). Celem tych ustaleń jest wybór odpowiedniej ścieżki rozwiązywania problemu - z udziałem specjalistów (lekarzy, terapeutów) lub bez – wyłącznie w szkole. W początkowej fazie popadania w uzależnienie do Internetu należy koncentrować się na wsparciu udzielonym w rodzinie i w szkole (psycholog/pedagog szkolny, wychowawca).
Aktywności wobec ofiar zdarzenia	Osoba, której problem dotyczy, powinna zostać otoczona zindywidualizowaną opieką przez pedagoga/psychologa szkolnego. Pierwszym jej etapem będzie rozmowa (rozmowy) ze specjalistą, która pozwoli zdiagnozować poziom zagrożenia, określić przyczyny popadnięcia w nałóg (np. sytuacja domowa, brak sukcesów edukacyjnych w szkole, izolacja w środowisku rówieśniczym) i ukazać specyfikę przypadku. Każde dziecko, u którego podejrzewa się nałóg korzystania z Internetu powinno zostać profesjonalnie zdiagnozowane przez psychologa szkolnego. Czasem warto w tym zakresie skorzystać z pomocy Poradni Psychologiczno-Pedagogicznej. Dziecku w trakcie wsparcia należy zapewnić komfort psychiczny - o jego sytuacji i specyfice uwarunkowań osobistych muszą zostać powiadomieni wszyscy uczący go i oceniający nauczyciele. O ile nie wiedzą o problemie swojego dziecka, niezbędne jest powiadomienie rodziców lub opiekunów prawnych dziecka i omówienie z nimi wspólnych rozwiązań. Tylko synergiczne współdziałanie rodziców i szkoły może zagwarantować powodzenie podejmowanych działań wspierających dziecko.
Aktywności wobec świadków zdarzenia	Jeśli świadkami problemu są rówieśnicy dziecka, należy im w rozmowie zwrócić uwagę

	na negatywne aspekty nadmiernego korzystania z zasobów Internetu oraz zaapelować o codzienne wsparcie dla dziecka dotkniętego problemem, a także o informowanie wychowawcy w przypadku wystąpienia kolejnych przypadków u innych dzieci.
Współpraca ze służbami i placówkami specjalistycznymi	W przypadku zdiagnozowania przez psychologa zaawansowanego uzależnienia od korzystania z zasobów Internetu dziecko powinno zostać skierowane przez szkołę, w bliskiej współpracy z rodzicami, do placówki specjalistycznej oferującej program terapeutyczny z zakresu przeciwdziałania uzależnieniom. W części przypadków może się okazać konieczna diagnoza i terapia lekarska.

5.Nawiązywanie niebezpiecznych kontaktów w Internecie - uwodzenie, zagrożenie pedofilią – procedura reagowania

Podstawy prawne uruchomienia procedury	Kodeks Karny, art. 200, 200a par 1 i 2, art. 286 par.1
Rodzaj zagrożenia objętego procedurą (opis)	Zagrożenie obejmuje kontakty osób dorosłych z małoletnimi w celu zainicjowania znajomości prowadzących do wyłudzenia poufnych informacji, nawiązania kontaktów seksualnych, skłonienia dziecka do zachowań niebezpiecznych dla jego zdrowia i życia lub wyłudzenia własności (np. danych, pieniędzy, cennych przedmiotów rodzinnych).
Telefony alarmowe krajowe	Telefon Zaufania dla Dzieci i Młodzieży - 116 111 Telefon dla Rodziców i Nauczycieli w sprawie Bezpieczeństwa Dzieci – 800 100 100 Zgłaszanie nielegalnych treści: Dyżurnet, dyzurnet.pl
SPOSÓB POSTĘPOWANIA W PRZYPADKU WYSTĄPIENIA ZAGROŻENIA	
Przyjęcie zgłoszenia i ustalenie okoliczności zdarzenia	Osobami najczęściej zgłaszającymi omawiany problem są rodzice/opiekunowie prawni dziecka lub osoby zajmujące się „poszukiwaniem pedofili”. W pierwszym przypadku informacja trafia najpierw do szkół, w drugim - na Policję. Zdarza się, że informacja uzyskiwana jest ze środowiska rówieśników ofiary. Kluczowe znaczenie w działaniach szkoły ma czas reakcji - szybkość przeciwdziałania zagrożeniu ze względu na niezwykle szkodliwe konsekwencje realizacji kontaktu online, przeradzającego się w zachowania w świecie rzeczywistym: uwiedzenie i wykorzystanie

	seksualne, kidnaping, a także wyłudzenie pieniędzy czy przedmiotów dużej wartości. W przypadkach niebezpiecznych kontaktów inicjowanych w Internecie może dochodzić do zagrożenia życia i zdrowia dziecka, szantażu i przymusu realizacji czynności seksualnych.
Opis okoliczności, analiza, zabezpieczenie dowodów	Reakcja szkoły powinna polegać w pierwszych krokach na ustaleniu skutków zdrowotnych i psychicznych, jakie nadmierne korzystanie z zasobów Internetu wywołało u dziecka (np. gorsze oceny w nauce, niedosypianie, niedojadanie, rezygnacja z dawnych zainteresowań, załamanie się relacji z rodziną czy rówieśnikami). Celem tych ustaleń jest wybór odpowiedniej ścieżki rozwiązywania problemu - z udziałem specjalistów (lekarzy, terapeutów) lub bez – wyłącznie w szkole. W początkowej fazie popadania w uzależnienie do Internetu należy koncentrować się na wsparciu udzielonym w rodzinie i w szkole (psycholog/pedagog szkolny, wychowawca).
Identyfikacja sprawcy(-ów)	Ze względu na bezpieczeństwo nie należy podejmować samodzielnych działań w celu dotarcia do sprawcy, lecz udzielać wszelkiego możliwego wsparcia organom ścigania, m.in. zabezpieczyć i przekazać zebrane dowody. Identyfikacja sprawcy wykracza poza kompetencje i możliwości szkoły w większości przypadków uwodzenia przez Internet.
Aktywności wobec sprawców ze szkoły/ spoza szkoły	Nie należy podejmować aktywności zmierzających bezpośrednio do kontaktu ze sprawcą. Zadaniem szkoły jest zebranie dowodów i opieka nad ofiarą i ew. świadkami.
Aktywności wobec ofiar zdarzenia	W każdym przypadku próby nawiązania niebezpiecznego kontaktu – np. w celu werbunku do sekty lub grupy promującej niebezpieczne zachowania, a także werbunku do grupy terrorystycznej należy przed wszystkim zapewnić ofierze opiekę psychologiczną i poczucie bezpieczeństwa. Podobne wsparcie winno być udzielone w przypadku zaobserwowania antyzdrowotnych i zagrażających życiu zachowań uczniów (samookaleczenia, zażywanie substancji psychoaktywnych), bowiem zachowania te mogą być inicjowane i wzmacniane poprzez kontakty w Internecie. O możliwym związku takich zachowań dzieci z inspiracją w Internecie należy powiadomić rodziców. Pierwszą czynnością w ramach reakcji na zagrożenie jest otoczenie ofiary pomocą psychologiczno-

	pedagogiczną we współpracy szkoły z rodzicami/opiekunami prawnymi. W trakcie rozmowy z dzieckiem prowadzonej w warunkach komfortu psychicznego przez wychowawcę/ pedagoga/psychologa/osobę ze szkoły, do której dziecko ma szczególne zaufanie, należy uzyskać wszelkie możliwe informacje o sprawcy i przekazać je Policji. Należy upewnić się, że kontakt ofiary ze sprawcą został przerwany, a dziecko odzyskało poczucie bezpieczeństwa. Towarzyszyć temu powinna analiza sytuacji domowej (rodzinnej) dziecka, w której tkwić może źródło poszukiwania kontaktów w Internecie. Dziecku należy udzielić profesjonalnej opieki terapeutycznej i/lub lekarskiej. Wszelkie działania szkoły wobec dziecka winny być uzgadniane z rodzicami/opiekunami prawnymi i inicjowane za ich zgodą.
Aktywności wobec świadków	Jeżeli zgłaszającym zagrożenie był rówieśnik ofiary, należy również objąć go opieką psychologiczną, pozytywnie wzmacniając jego reakcję na zdarzenie.
Współpraca z Policją i sądami rodzinnymi	W przypadkach naruszenia prawa – szczególnie w przypadku uwiedzenia dziecka do lat 15 – obowiązkiem szkoły jest powiadomienie Policji lub sądu rodzinnego.
Współpraca ze służbami społecznymi i placówkami specjalistycznymi	W przypadkach uwiedzenia nieletnich przez osoby dorosłe rekomenduje się – w porozumieniu z rodzicami/opiekunami prawnymi – skierowanie ofiary na terapię do placówki specjalistycznej opieki psychologicznej.

6.Seksting, prowokacyjne zachowania i aktywność seksualna jako źródło dochodu osób nieletnich – procedura reagowania

Podstawy prawne uruchomienia procedury	Kodeks Karny, art. 191a i 202
Rodzaj zagrożenia objętego procedurą (opis)	Seksting to przesyłanie drogą elektroniczną w formie wiadomości MMS lub publikowanie np. w portalach (społecznościowych) prywatnych treści, głównie zdjęć, o kontekście seksualnym, erotycznym i intymnym.
SPOSÓB POSTĘPOWANIA W PRZYPADKU WYSTĄPIENIA ZAGROŻENIA	
Przyjęcie zgłoszenia i ustalenie okoliczności zdarzenia	Zgłoszeń przypadków sekstingu dokonują głównie rodzice lub opiekunowie prawni dziecka - ofiary. Czasami informacja dociera do szkoły bezpośrednio od jej samej lub z grona bliskich znajomych dziecka. W rzadkich

	wypadkach nauczyciele i inni pracownicy szkoły sami identyfikują takie zdarzenia w sieci. Delikatny charakter sprawy, a także potencjalna penalizacja sprawcy, wymagają zachowania daleko posuniętej dyskrecji i profesjonalnej reakcji. Czasami zgłoszenia dokonują ofiary lub osoby je znające.
Opis okoliczności, analiza, zabezpieczenie dowodów	Wyróżniamy 3 podstawowe rodzaje sekstingu, które skutkują koniecznością realizacji zmodyfikowanych procedur reagowania: Rodzaj 1. Wymiana materiałów o charakterze seksualnym następuje tylko w ramach związku między dwojgiem rówieśników. Materiały nie uległy rozprzestrzenieniu dalej. Rodzaj 2. Materiały o charakterze seksualnym zostały rozesłane większej liczbie osób, jednak nie dochodzi do cyberprzemocy na tym tle. Młodzież traktuje materiał jako formę wyrażenia siebie. Rodzaj 3. Materiały zostały rozesłane większej liczbie osób w celu upokorzenia osoby na nich zaprezentowanej – lub zostają rozpowszechnione omyłkowo, jednak są zastosowane jako narzędzie cyberprzemocy
Identyfikacja sprawcy(-ów)	Identyfikacja sprawcy będzie możliwa przede wszystkim dzięki zabezpieczeniu dowodów - przesyłanych zdjęć, czy zrzutów ekranów portali, w których opublikowano zdjęcie(-a). Jako, że seksting jest karalny, skrupulatność i wiarygodność dokumentacji ma duże znaczenie. Należy przy tym przestrzegać zasad dyskrecji, szczególnie w środowisku rówieśniczym ofiary.
Aktywności wobec sprawców ze szkoły/ spoza szkoły	Zidentyfikowani małoletni sprawcy sekstingu winni zostać wezwani do dyrekcji szkoły, gdzie zostaną im przedstawione dowody ich aktywności. Niezależnie od zakresu negatywnych zachowań i działań wszyscy sprawcy powinni otrzymać wsparcie pedagogiczne i psychologiczne. Konieczne są także rozmowy ze sprawcami w obecności ich rodziców zaproszonych do szkoły. Rodzaj 1. Dalsze działania poza zapewnieniem wsparcia i opieki psychologicznopedagogicznej nie są konieczne, jednak istotne jest pouczenie sprawców zdarzenia, że dalsze rozpowszechnianie materiałów może być nielegalne i będzie miało ostrzejsze konsekwencje, w tym prawne. Rodzaj 2. Niektóre z tego typu materiałów mogą zostać uznane za pornograficzne, w takim wypadku na dyrektorze placówki ciąży obowiązek zgłoszenia

	incydentu na Policję. Rozpowszechnianie materiałów pornograficznych z udziałem nieletnich jest przestępstwem ściganym z urzędu (par. 2020 Kodeksu Karnego), dlatego też dyrektor placówki jest zobowiązany do zgłoszenia incydentu na Policję i/lub do sądu rodzinnego. Wszelkie działania wobec sprawców incydentu powinny być podejmowane w porozumieniu z ich rodzicami lub opiekunami prawnymi. Rodzaj 3. Niektóre z tego typu materiałów mogą zostać uznane za pornograficzne – konieczne zgłoszenie takiego przypadku na Policję. W sytuacji zaistnienia znamion cyberprzemocy, należy dodatkowo zastosować procedurę: Cyberprzemoc. Decyzja o ewentualnym poinformowaniu opiekunów powinna być podejmowana przez pedagoga/psychologa, biorącego pod uwagę dobro małoletnich, w zależności od charakteru sytuacji.
Aktywności wobec ofiar zdarzenia	Pierwszą reakcją szkoły i rodziców, obok dokumentacji dowodów, winno być otoczenie wszechstronną, dyskretną opieką psychologiczno - pedagogiczną ofiary oraz zaproponowanie odpowiednich działań wychowawczych, w przypadku upublicznienia przypadku sekstingu w środowisku rówieśniczym. Rozmowa na temat identyfikacji potencjalnego sprawcy powinna być realizowana w warunkach komfortu psychicznego dla dziecka – ofiary sekstingu, z szacunkiem dla jego indywidualności i przeżytego stresu.
Aktywności wobec świadków	Jeśli przypadek sekstingu zostanie upowszechniony w środowisku rówieśniczym – np. poprzez przesłanie MMS do uczniów tej samej szkoły lub klasy lub publikację w portalu społecznościowym, należy podjąć działania wychowawcze, uświadamiające negatywne aspekty moralne sekstingu oraz narażanie się na dotkliwe kary.
Współpraca z Policją i sądami rodzinnymi	W przypadku publikacji lub upowszechniania zdjęć o charakterze pornografii dziecięcej (co jest wykroczeniem ściganym z urzędu) kierownictwo szkoły jest zobowiązane do powiadomienia o tym zdarzeniu Policji lub sądu rodzinnego.
Współpraca ze służbami społecznymi i placówkami specjalistycznymi	Kontakt ofiar z placówkami specjalistycznymi może okazać się konieczny w indywidualnych przypadkach. O skierowaniu do nich decyzję powinien podjąć psycholog/pedagog szkolny

	wspólnie z rodzicami/opiekunami prawnymi ofiary.

7.Bezkrytyczna wiara w treści zamieszczone w Internecie, nieumiejętność odróżnienia treści prawdziwych od nieprawdziwych, szkodliwość reklam – procedury reagowania

Podstawy prawne uruchomienia procedury	Ustawa z 11 stycznia 2017r. – prawo oświatowe
Rodzaj zagrożenia objętego procedurą (opis)	Brak umiejętności odróżniania informacji prawdziwych od nieprawdziwych publikowanych w Internecie, bezkrytyczne uznawanie za prawdę tez publikowanych w forach internetowych, kierowanie się informacjami zawartymi w reklamach. Taka postawa dzieci prowadzić może do zagrożeń życia i zdrowia (np. stosowania wyniszczającej diety, samookaleczeń), skutkować rozczarowaniami i porażkami życiowymi (w efekcie korzystania z fałszywych informacji), utrudniać lub uniemożliwiać osiąganie dobrych wyników w edukacji (korzystanie z upraszczających i zawężających temat „ściąg" i „bryków"), a także utrwalenia się u ucznia ambiwalentnych postaw moralnych.
SPOSÓB POSTĘPOWANIA W PRZYPADKU WYSTĄPIENIA ZAGROŻENIA	
Przyjęcie zgłoszenia i ustalenie okoliczności zdarzenia	Uczniowie nie umiejący odróżniać prawdy od fałszu informacji publikowanych w Internecie winni być identyfikowani przez nauczycieli i wychowawców w trakcie lekcji wszystkich przedmiotów. Często taka postawa ujawnia się podczas przygotowania prac domowych i jest stosunkowo łatwa do zidentyfikowania przez oceniającego nauczyciela.
Opis okoliczności, analiza, zabezpieczenie dowodów	Posługiwanie się nieprawdziwymi informacjami zaczerpniętymi z Internetu w procesie dydaktycznym – podczas lekcji lub w zadaniach domowych, każdorazowo winno być zauważone przez nauczyciela, przeanalizowane i sprostowane. Przypadki spektakularne powinny być archiwizowane przez nauczycieli i wykorzystywane podczas zajęć z edukacji medialnej (informacyjnej).
Aktywności wobec ofiar zdarzenia	Szkoła powinna prowadzić działania profilaktyczne - edukację medialną (informacyjną), zarówno w formie zajęć pozalekcyjnych, jak i w trakcie lekcji przedmiotów nieinformatycznych (np. historii, języka polskiego, wychowania w rodzinie) przez wszystkie lata nauki ucznia w szkole. Zajęcia w szkole mogą mieć charakter kilkuminutowych elementów edukacji medialnej wplecionej w lekcje o innej tematyce i/lub lekcji

	ukierunkowanych na zdobywanie przez dzieci i młodzież kompetencji medialnych

8.Zagrożenia bezpieczeństwa technicznego sieci, komputerów i zasobów online – procedura reagowania

Podstawy prawne uruchomienia procedury	Ustawa z dnia 14 grudnia 2016 r. - Prawo oświatowe, Statut szkoły
Rodzaj zagrożenia objętego procedurą (opis)	Kategoria technicznych zagrożeń bezpieczeństwa cyfrowego obejmuje obecnie szerokie spectrum problemów: (1) ataki przez wirusy, robaki i trojany, (2) ataki na zasoby sieciowe (hakerstwo, spyware, crimeware, eksploit, ataki słownikowe i back door, skanowanie portów, phishing, pharming, sniffing, spoofing, ataki Denial of service (DoS), rootkit) i ataki socjotechniczne. Na styku z zagadnieniami technicznymi lokalizują się zagrożenia wynikające z nieprawidłowych i szkodliwych zachowań użytkowników, np. używanie łatwych do odgadnięcia haseł, pozostawianie komputerów włączonych bez opieki, czy brak zabezpieczeń na wypadek braku energii elektrycznej.
SPOSÓB POSTĘPOWANIA W PRZYPADKU WYSTĄPIENIA ZAGROŻENIA	
Przyjęcie zgłoszenia i ustalenie okoliczności zdarzenia	W przypadku wystąpienia incydentów zagrożenia bezpieczeństwa cyfrowego pracownik szkoły zobowiązany jest do zgłoszenia go osobie odpowiedzialnej za infrastrukturę cyfrową szkoły oraz dyrekcji. Kluczowe znaczenie ma zebranie i zabezpieczenie przez specjalistę dowodów w formie elektronicznej.
Opis okoliczności, analiza, zabezpieczenie dowodów	W części przypadków szkoła poradzi sobie we własnym zakresie, w niektórych konieczne będzie skorzystanie z zewnętrznego wsparcia wyspecjalizowanych firm.
Identyfikacja sprawcy(-ów)	Identyfikację sprawców ataku należy pozostawić specjalistom – informatykom. W sytuacji, gdy incydent spowodował szkole straty materialne lub wiązał się z utratą danych należy powiadomić Policję, aby podjęła działania na rzecz zidentyfikowania sprawcy.
Aktywności wobec sprawców ze szkoły/ spoza szkoły	Jeśli sprawcami incydentu są uczniowie danej szkoły, o zaistniałej sytuacji należy powiadomić ich rodziców, zaś wobec nich podjąć działania wychowawcze. Jeżeli skutki ataku mają dotkliwy charakter, doprowadziły do zniszczenia mienia lub utraty istotnych danych (np. gromadzonych w e-dzienniku szkoły), należy taki przypadek zgłosić na Policję

Aktywności wobec świadków	O incydencie należy powiadomić społeczność szkolną (uczniów, nauczycieli, rodziców) i zaprezentować podjęte sprawnie działania, tak przywracające działanie aplikacji i sieci komputerowej w szkole, jak i wychowawczo-edukacyjne wobec dzieci.
Współpraca z Policją i sądami rodzinnymi	W przypadku wystąpienia strat materialnych oraz utraty danych (szczególnie danych wrażliwych) należy zgłosić incydent na Policji.
Współpraca ze służbami społecznymi i placówkami specjalistycznymi	W przypadkach zaawansowanych awarii (np. wywołanych przez trojany) lub strat (np. utrata danych) konieczne jest skorzystanie z zewnętrznego wsparcia eksperckiego, kontakt z serwisem twórcy oprogramowania lub zamówienie usługi w wyspecjalizowanej firmie.