Załącznik nr 10. Procedury ochrony dzieci przed treściami szkodliwymi i zagrożeniami w sieci Internet

PROCEDURA

ochrony dzieci przed treściami szkodliwymi i zagrożeniami w sieci Internet w Przedszkolu Publicznym w Tułowicach

Podstawa prawna:

- art. 22c ust. 2 pkt 3 ustawy z dnia 13 maja 2016 r. o przeciwdziałaniu zagrożeniom przestępczością na tle seksualnym i ochronie małoletnich (tekst jedn.: Dz.U. z 2023 r. poz. 1304 ze zm.)

§ 1

Cel procedury

Celem niniejszej Procedury jest:

1) stosowanie standardów ochrony małoletnich przyjętych w Przedszkolu, w szczególności standardu bezpieczeństwa cyfrowego;
2) przedstawienie pakietu podstawowych działań na rzecz zapewnienia bezpieczeństwa małoletnich w środowisku cyfrowym, jakie powinny zostać podjęte w Przedszkolu.

§ 2

Postanowienia ogólne

1. Niniejsza Procedura określa:

1) zasady postępowania pracowników przedszkola w przypadku ochrony dzieci przed treściami szkodliwymi i zagrożeniami w sieci Internet;

2) podstawowe działania przedszkola na rzecz bezpieczeństwa cyfrowego;

3) procedury na wypadek wystąpienia zagrożeń bezpieczeństwa cyfrowego w przedszkolu.

2. Proponowane działania profilaktyczne są odpowiedzią na obowiązek: „upowszechniania wśród dzieci i młodzieży wiedzy o bezpieczeństwie oraz kształtowania właściwych postaw wobec zagrożeń, w tym związanych z korzystaniem z technologii informacyjno-komunikacyjnych”, który nakłada na szkoły ustawa z 14 grudnia 2016 r. – Prawo oświatowe.

3. Ilekroć w Procedurze jest mowa o:

1) **placówce** – należy przez to rozumieć przedszkole;

2) **dziecku, małoletnim** – należy przez to rozumieć wychowanka uczęszczającego do przedszkola;

§ 3

Podstawowe działania przedszkola na rzecz bezpieczeństwa cyfrowego w przedszkolu

1. Zagrożenia bezpieczeństwa cyfrowego w przedszkolu oraz problemy dziecka w świecie cyfrowym mogą mieć różnorodny charakter. W przypadkach wystąpienia incydentu naruszenia bezpieczeństwa cyfrowego, zwłaszcza wobec naruszenia prawa, działania placówki cechuje otwartość w działaniu, szybka identyfikacja problemu - określenie szkodliwych lub niezgodnych z prawem zachowań - i jego rozwiązywanie adekwatnie do poziomu zagrożenia, jakie wywołało.
2. W przypadku dostępu realizowanego pod nadzorem pracownika placówki, ma on obowiązek informowania dzieci o zasadach bezpiecznego korzystania z Internetu. Pracownik placówki czuwa także nad bezpieczeństwem korzystania z Internetu.

§ 4

Procedura postępowania w przypadku zagrożenia bezpieczeństwa technicznego sieci, komputerów i zasobów

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,DDoS 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.

Podstawa prawna uruchomienia procedury
Ustawa z dnia 14 grudnia 2016 r. Prawo oświatowe. Kodeks karny, Rozdział XXXIII Przestępstwa przeciwko ochronie informacji: art. 267 § 1–4, art. 268 § 1–3, art. 268a § 1–2, art. 269 § 1–2, art. 269a, art. 269b § 1–2 Kodeks cywilny: art. 415.

Sposób postępowania w przypadku wystąpienia zagrożenia	
Przyjęcie zgłoszenia i ustalenie okoliczności zdarzenia	W przypadku wystąpienia incydentów zagrożenia bezpieczeństwa cyfrowego pracownik przedszkola zobowiązany jest do zgłoszenia go osobie odpowiedzialnej za infrastrukturę cyfrową –dyrektorowi przedszkola. Kluczowe znaczenie ma zebranie i zabezpieczenie przez specjalistę dowodów w formie elektronicznej.
Opis okoliczności, analiza, zabezpieczenie dowodów	Szczegółowy opis procedur reagowania na wystąpienie w przedszkolu różnorodnych zagrożeń bezpieczeństwa cyfrowego powinien zostać zawarty w dokumencie „Instrukcji zarządzania systemem informatycznym" danej placówki. W części przypadków przedszkole 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 straty materialne lub wiązał się z utratą danych należy powiadomić Policję, aby podjęła działania na rzecz zidentyfikowania sprawcy.
Aktywności wobec świadków	O incydencie należy powiadomić nauczycieli i zaprezentować podjęte sprawnie działania przywracające działanie aplikacji i sieci komputerowej w przedszkolu.
Współpraca z Policją	W przypadku wystąpienia strat materialnych oraz utraty danych (szczególnie danych wrażliwych) należy zgłosić incydent na Policji, UODO.
Współpraca z 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.

§ 5

Postanowienia końcowe

1. Niniejsza procedura wchodzi w życie z dniem 01.03.2024r.

2. Za zamieszczanie oraz informowanie o aktualnej treści procedury odpowiada dyrektor przedszkola.