POLITYKA BEZPIECZEŃSTWA CYFROWEGO

w Szkole Podstawowej Nr 15 im. Armii Krajowej w Elblągu

I. Postanowienia wstępne

Polityka cyberbezpieczeństwa jest zbiorem zasad i procedur mających na celu ochronę informacji i systemów informatycznych szkoły przed zagrożeniami cyfrowymi. Celem tego dokumentu jest zapewnienie, że wszyscy członkowie społeczności szkolnej są świadomi swojej roli w utrzymaniu bezpieczeństwa cyfrowego.

II. Ilekroć w dokumencie jest mowa o:

1) sieci – rozumie się przez to sieć telekomunikacyjną, wykorzystywaną głównie do świadczenia publicznie dostępnych usług telekomunikacyjnych,
2) systemie informatycznym – rozumie się przez to zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych,
3) szkole – rozumie się przez to Szkołę Podstawową Nr 15 im. Armii Krajowej w Elblągu,
4) użytkowniku – rozumie się przez to uczniów i nauczycieli korzystających z dostępnych w szkole sieci internetowych,
5) cyberprzemocy (agresja elektroniczna) – rozumie się przez to stosowanie przemocy poprzez: prześladowane, zastraszanie, nękanie, wyśmiewanie innych osób z wykorzystaniem Internetu i narzędzi typu elektronicznego takich jak sms, witryny internetowe, fora dyskusyjne w Internecie i inne.

III. Zakres

Polityka dotyczy wszystkich uczniów, nauczycieli, pracowników administracyjnych i innych osób korzystających z systemów informatycznych szkoły.

IV. Działania profilaktyczne

Działanie	Opis	Osoba odpowiedzialna
Opracowanie, realizacja i aktualizacja szkolnych działań mających na celu zapewnienia bezpieczeństwa cyfrowego	Ustalenie zasad dotyczących korzystania z systemów informatycznych szkoły, w tym zasad dotyczących haseł, instalacji oprogramowania	Dyrektor szkoły, nauczyciel informatyki

	i etykiety w sieci.	
Szkolenia	Organizowanie szkoleń dla pracowników oraz zajęć dydaktycznych dla uczniów dotyczących cyberbezpieczeństwa	Nauczyciel informatyki, zewnętrzny specjalista ds. bezpieczeństwa
Monitorowanie	Regularne monitorowanie systemów informatycznych szkoły w celu wykrywania potencjalnych zagrożeń i naruszeń polityki.	Administrator systemu, nauczyciel informatyki
Reagowanie na naruszenia	Podejmowanie odpowiednich działań w przypadku naruszeń polityki, w tym zawieszania dostępu do systemów informatycznych szkoły i podejmowania działań prawnych w przypadku poważnych naruszeń.	Dyrektor szkoły, administrator systemu
Przegląd polityki	Regularne przeglądanie i aktualizowanie polityki, aby zapewnić jej skuteczność i zgodność z najnowszymi standardami bezpieczeństwa cyfrowego	Dyrektor szkoły, nauczyciel informatyki, administrator systemu

V. Zasady

1) Należy używać tylko silnych, indywidualnych dla każdego systemu haseł i nie udostępnianie ich nikomu.
2) Należy używać oprogramowania antywirusowego. Stosowanie ochrony w czasie rzeczywistym.
3) Należy aktualizować oprogramowanie antywirusowe oraz bazy danych wirusów.
4) Należy regularnie aktualizować system operacyjny i aplikacje.
5) Nie należy otwierać plików nieznanego pochodzenia.

6) Zakazuje się korzystania ze stron internetowych (zwłaszcza ze stron banków, poczty elektronicznej czy portali społecznościowych), które nie mają ważnego certyfikatu SSL.
7) Zakazuje się korzystania z niesprawdzonych programów zabezpieczających.
8) Należy regularnie skanować komputer i sprawdzać zachodzące procesy sieciowe.
9) Należy sprawdzać pliki pobrane z Internetu za pomocą programu antywirusowego.
10) Należy unikać odwiedzania stron, które oferują wyjątkowe atrakcje (darmowe filmiki, darmową muzykę).
11) Nie należy wpisywać danych osobowych w niesprawdzonych serwisach.
12) Należy pamiętać, iż żaden bank czy urząd nie wysyła e-maili do swoich klientów z prośbą o podanie hasła lub loginu w celu ich weryfikacji.

VI. Procedury reagowania w przypadku wystąpienia w szkole zagrożeń bezpieczeństwa cyfrowego

1) Działania wobec aktu / zdarzenia – opis przypadku, ustalenie okoliczności zdarzenia, zabezpieczenie dowodów oraz monitoring sytuacji szkolnej. Należy pamiętać o zachowaniu (nieusuwaniu) dokumentacji cyfrowej: wiadomości sms, e-maili, nagrań z poczty głosowej telefonu, komentarzy w serwisie społecznościowym, zapisów na blogu czy plików filmów wideo. Każde zdarzenie wymaga udokumentowania w stosownym protokole.
2) Działania wobec uczestników zdarzenia - oznaczają te aktywności, które podejmowane są wobec ofiar (osób poszkodowanych), sprawców i świadków zdarzenia. W przypadku gdy osobami poszkodowanymi są osoby nieletnie kolejną grupą pośrednich uczestników zdarzenia są rodzice.
3) Standardowa procedura reakcji na zagrożenie bezpieczeństwa cyfrowego powinna przebiegać wg schematu:
   a) Rozmowa uczestnika zdarzenia z dyrekcją szkoły.
   b) Powiadomienie rodziców poszkodowanego.
   c) Działania wychowawcze i wyciągnięcie konsekwencji wobec sprawcy.
   d) Powiadomienie policji / sądu rodzinnego w przypadku naruszenia prawa.
   e) Udzielenie uczestnikom wsparcia psychologicznego.
4) Działania wobec instytucji / organizacji / służb pomocowych i współpracujących. Współpraca z zewnętrznymi instytucjami jest niezbędna w przypadku naruszenia przepisów prawa przez uczniów lub osoby spoza szkoły. Szkoła współpracuje z:

- policją i sądami rodzinnymi,
- służbami społecznymi i placówkami specjalistycznymi,
- dostawcami usług internetowych oraz operatorami telekomunikacyjnymi.

5) Sprawców wszystkich rodzajów zagrożeń bezpieczeństwa cyfrowego w szkole należy objąć poniższymi działaniami:
   a) Sprawca musi otrzymać komunikat o braku akceptacji dla działań jakich dokonał, poznać możliwe skutki i konsekwencje swojego postępowania (np. wynikające ze Statutu Szkoły). Powinien zostać wezwany do zaprzestania podejmowania podobnych działań w przyszłości oraz usunięcia skutków swoich dotychczasowych działań (np. publikacji na portalu społecznościowym). Sprawcę należy objąć pomocą psychologiczno-pedagogiczną, by podobne zdarzenia nie miały miejsca w przyszłości. W przypadku, kiedy sprawców jest więcej, należy z każdym z nich rozmawiać osobno.
   b) Decyzję o karze dla sprawcy, powinna podejmować rada pedagogiczna (po poznaniu wszystkich okoliczności zdarzenia), a przekazywać Dyrektor Szkoły.
   c) Podejmując decyzję o zastosowaniu sankcji, należy wziąć pod uwagę:
      - rozmiar i rangę szkody 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.;
      - czas trwania prześladowania – czy było to długotrwałe działanie, czy pojedynczy incydent;
      - świadomość popełnianego czynu – czy działanie było zaplanowane, a sprawca był świadomy, że postąpił nagannie, czy wie, że wyrządził krzywdę koledze. Należy również zwrócić uwagę na to jak wiele wysiłku włożył w ukrycie swojej tożsamości itp.;
      - motywacje sprawcy – należy sprawdzić, czy działanie sprawcy nie jest działaniem odwetowym w odpowiedzi na uprzednie doświadczenia sprawcy.
   d) Rodzice muszą zostać powiadomieni o zdarzeniu oraz zapoznani z materiałami i decyzją co do dalszego postępowania ze sprawcą (np. z zastosowanymi sankcjami). Powinni oni również zostać poinformowani, iż rodzice ofiary mają prawo zgłosić sprawę policji. Jeśli sprawcą czynu jest osoba spoza szkoły, należy

zapewnić bezpieczeństwo ofierze i poinformować ją i jej rodziców o przysługujących jej prawach.

VII. Postanowienia końcowe

Szkoła Podstawowa Nr 15 im. Armii Krajowej w Elblągu zobowiązuje się do spełnienia wymagań zewnętrznych i wewnętrznych oraz zapewnia, że założenia niniejszej Polityki Cyberbezpieczeństwa są znane i zrozumiałe dla pracowników oraz uczniów. Zasoby na jej realizację zabezpieczono.