.....
(pieczęć firmowa)

Polityka dziennika elektronicznego

Spis treści

1. Wstęp....1
2. Informacje wstępne....1
3. Dostęp do dziennika elektronicznego....2
4. Zasady bezpieczeństwa....2
4.1. Bezpieczeństwo hasła....2
4.2. Bezpieczeństwo komputera....3
5. Szczególne przypadki....4

1. Wstęp

1. Niniejszy dokument jest częścią zbioru polityk bezpieczeństwa.
2. Definicje pojęć i podstawa prawna zostały opisane w pierwszych rozdziałach ww Zbioru.

2. Informacje wstępne

1. Administrator wprowadził w Placówce dziennik elektroniczny.
2. Dziennik elektroniczny został wprowadzony na podstawie § 8 ust. 1 rozporządzenia Ministra Edukacji Narodowej z 25 sierpnia 2017 r. w sprawie sposobu prowadzenia przez publiczne przedszkola, szkoły i placówki dokumentacji przebiegu nauczania, działalności wychowawczej i opiekuńczej oraz rodzajów tej dokumentacji (dalej „rozporządzenie w sprawie dokumentacji”) wydanego do ustawy z 14 grudnia 2016 r. - Prawo oświatowe.
3. Przetwarzanie danych w dzienniku elektronicznym, analogicznie jak przetwarzanie danych w dzienniku papierowym, odbywa się na mocy przepisów prawa (art. 6 ust. 1 lit. c RODO).
4. Z dostawcą dziennika elektronicznego Administrator zawarł umowę przetwarzania danych zgodną z art. 28. RODO.

3. Dostęp do dziennika elektronicznego

1. Dziennikiem zarządza administrator dziennika wyznaczony przez Administratora. Zajmuje się on tworzeniem kont oraz konfigurowaniem parametrów działania dziennika. Administrator prowadzi aktualny spis administratorów dziennika w dokumentacji ochrony danych.
2. Każdy użytkownik dziennika elektronicznego posiada własne konto, za które osobiście odpowiada.
3. W dzienniku występują 4 główne kategorie kont:
   a) konta administracji szkolnej
   b) konta nauczycieli
   c) konta uczniowskie
   d) konta rodziców
4. Administratorzy dziennika są zobowiązani do takiej konfiguracji kont, aby użytkownicy mieli oni dostęp wyłącznie do danych, do których są uprawnieni.
5. Każdy użytkownik otrzymuje od Administratora login i hasło służące do pierwszego logowania. Login jednoznacznie identyfikuje użytkownika i nie zostanie przydzielony innemu użytkownikowi, nawet po ustaniu aktywności konta.
6. Każdy użytkownik jest zobowiązany do przestrzegania zasad niniejszej polityki, także użytkownicy kont rodzicielskich oraz uczniowskich.

4. Zasady bezpieczeństwa

4.1. Bezpieczeństwo hasła

1. Hasło użytkownika stanowi tajemnicę i nie może być nikomu ujawniane, nawet innym użytkownikom o tych samych uprawnieniach. Tajemnicą objęte są również stare hasła, które uległy już zmianie na nowe.
2. Zabronione jest udostępnianie nie tylko hasła ale i konta. Każdy użytkownik pracuje z własnym kontem samodzielnie. Zabronione jest również udostępnianie kont rodzicielskich uczniom.
3. Użytkownik powinien przestrzegać zasad bezpieczeństwa hasła, takich jak:
   a) konieczność zmiany hasła za każdym razem, gdy występuje choć niewielkie podejrzenie, że obecne hasło mogło zostać poznane przez osobę nieuprawnioną;
   b) konieczność okresowej zmiany hasła, z częstotliwością zależną od miejsc użycia hasła:
      – nie rzadziej niż raz na kwartał przy wykorzystywaniu hasła wyłącznie na zaufanych komputerach w warunkach domowych,

- nie rzadziej niż raz na miesiąc przy wykorzystywaniu hasła wyłącznie na zaufanych komputerach w warunkach publicznych,
- nie rzadziej niż raz na tydzień przy wykorzystywaniu hasła na niezaufanych komputerach (np. w bibliotece szkolnej);

c) konieczność dobierania tzw. bezpiecznych haseł, czyli haseł

- stanowiących tzw. passphrase czyli zdanie składające się z kilku wyrazów, zawierających małe i duże litery, a także cyfry i znak specjalny, przykładowo *„Kto ma 2 uszy niechaj słucha!*[1]*”*
- różniących się od poprzednich haseł w sposób istotny,
- nie kojarzących się z właścicielem hasła.

d) zakaz zapisywania haseł w sposób jawny w miejscu niezabezpieczonym[2].

4.2. Bezpieczeństwo komputera

1. Wykorzystanie dziennika elektronicznego przez nauczycieli i administrację możliwe jest wyłącznie na zaufanych komputerach. Mogą to być komputery służbowe udostępnione przez Administratora do celów obsługi dziennika albo komputery domowe nauczycieli.
2. W przypadku kont uczniowskich i rodzicielskich dopuszcza się (choć zdecydowanie się tego nie zaleca) sporadyczne wykorzystanie konta na komputerach niezaufanych (biblioteka, komputery w pracy rodzica, etc.), jednak wtedy zaleca się częstą zmianę hasła.
3. W przypadku wykorzystywania konta na komputerach innych niż udostępnione przez Administratora do obsługi dziennika elektronicznego, pełną odpowiedzialność za bezpieczeństwo ponosi użytkownik konta. W szczególności powinien on zadbać o to, aby:
   a) Komputer nie był zawirusowany ani nie zawierał tzw. keyloggera (programu przechwytującego hasła). Dotyczy to również przeglądarki internetowej, która może zostać zawirusowana złośliwym dodatkiem[3].
   b) Przeglądarka nie miała aktywnej funkcji zapisywania hasła.
   c) Ułożenie klawiatury i monitora uniemożliwiało podejrzenie hasła przez osoby trzecie.
   d) Ułożenie monitora uniemożliwiało odczytanie danych przez osoby trzecie.
   e) Komputer nie znajdował się w trybie udostępniania pulpitu[4] (na przykład obsłudze serwisowej lub w czasie zdalnego nauczania).

[1] Oczywiście to hasło, z uwagi na jego publikacje w zasadach już się nie nadaje do użycia, jako hasło podane do publicznej wiadomości.

[2] Zaleca się stosowanie elektronicznych portfeli na hasła, takich jak KeyPass XC (https://keepassxc.org/) lub papierowych notatników na hasła zabezpieczonych w zamykanym sejfie, kasetce lub szafie pancernej.

[3] Złośliwe dodatki mogą działać niezależnie od systemu operacyjnego i nawet uznawane za bezpieczne systemy MacOS czy Linux nie zapewnią wtedy bezpieczeństwa danych.

f) System operacyjny komputera był zaktualizowany.

g) Po zakończeniu pracy nastąpiło wylogowanie z konta dziennika.

4. W przypadku jakichkolwiek wątpliwości do do bezpieczeństwa komputera, użytkownik zobowiązany jest zrezygnować z wykorzystania na nim dziennika elektronicznego.

4.3. Bezpieczeństwo wiadomości oraz załączników

1. Dziennik elektroniczny umożliwia przesyłanie wiadomości, których treść jest przechowywana w systemie dziennika i jest tak bezpieczna, jak bezpieczny jest sam dziennik oraz jak bezpiecznie zostało ochronione hasło.

2. Dziennik elektroniczny umożliwia dołączanie załączników do wiadomości, jednak są one przetwarzane poza systemem dziennika. Są one przetwarzane przez podmioty trzecie, zależne od dołączonego systemu chmurowego (OneDrive, Google Drive, Dropbox). W związku z tym:

   a) W przypadku kont nauczycieli i administracji szkolnej dopuszczalne jest dołączanie wyłącznie chmurowych dysków powiązanych ze służbowymi kontami, które powinny być chronione analogicznie jak konta dziennika.

   b) W przypadku kont uczniowskich, zaleca się podłączanie dysków szkolnych kont uczniowskich oraz nieprzesyłanie w załącznikach istotnych danych osobowych.

   c) W przypadku kont rodzicielskich zaleca się uważny dobór konta dostawcy chmurowego oraz unikanie przesyłania w załącznikach istotnych danych osobowych.

5. Postępowanie w przypadku naruszenia

1. W przypadku wykrycia naruszenia ochrony danych lub naruszenia bezpieczeństwa hasła, a także w przypadku jedynie podejrzenia takiego naruszenia, użytkownik zobowiązany jest do niezwłocznego zawiadomienia Administratora.

[4] Udostępnianie pulpitu jest wykorzystywane przez administratorów i serwisantów udzielających pomocy technicznej przy pomocy takich programów jak TeamViewer, AnyDesk, DW Service, LogMe In itp. Może być także aktywne podczas korzystania z narzędzi takich jak Meet, Teams, Zoom, Skype czy innych do prowadzenia zdalnego nauczania lub rozmów.