ZESPÓŁ SZKÓŁ
im. Bolesława Prusa w Pułtusku
ul. M. Konopnickiej 9
06-100 PUŁTUSK
tel./fax 23 692 22 42



**Szczegółowe warunki i zasady korzystania z technologii informacyjno-komunikacyjnej**

1. Każdy pracownik szkoły korzystający ze służbowego sprzętu IT zobowiązany jest do jego zabezpieczenia przed zniszczeniem lub uszkodzeniem. Za sprzęt IT przyjmuje się: komputery stacjonarne, monitory, drukarki, skanery, ksera, laptopy, tablety i smartfony.
2. Pracownik jest zobowiązany zgłosić dyrektorowi szkoły/placówki zagubienie, utratę lub zniszczenie powierzonego mu sprzętu IT.
3. Samowolne instalowanie otwieranie (demontaż) sprzętu IT, instalowanie dodatkowych urządzeń (np. twardych dysków, pamięci) lub podłączanie jakichkolwiek niezatwierdzonych urządzeń do systemu informatycznego jest zabronione.
4. Przed koniecznością czasowego opuszczenia stanowiska pracy, pracownik szkoły zobowiązany jest wylogować się z systemu bądź z programu.
5. Po zakończeniu pracy, pracownik szkoły zobowiązany jest:
   a) wylogować się z systemu informatycznego, a jeśli to wymagane - wyłączyć sprzęt komputerowy,
   b) zabezpieczyć stanowisko pracy, w szczególności wszelkie nośniki magnetyczne i optyczne, na których znajdują się dane osobowe.
6. Pracownik jest zobowiązany do usuwania plików z nośników/dysków, do których mają dostęp inni użytkownicy nieupoważnieni do dostępu do takich plików (np. podczas współużytkowania komputerów).
7. W trakcie kształcenia na odległość, w sytuacji, gdy nauczyciele korzystają ze swojego prywatnego sprzętu komputerowego, ponoszą odpowiedzialność za bezpieczeństwo danych osobowych uczniów, rodziców, innych nauczycieli oraz pracowników szkoły, które gromadzą i są zobowiązani do przestrzegania procedur określonych w polityce ochrony danych osobowych.

**Zarządzanie uprawnieniami – procedura rozpoczęcia, zawieszenia i zakończenia pracy zdalnej**

8. Każdy nauczyciel i każdy uczeń – zwany dalej użytkownikiem (np. komputera stacjonarnego, laptopa, dysku sieciowego, programów, w których pracuje, poczty elektronicznej) musi posiadać swój własny indywidualny identyfikator (login) do logowania się.
9. Zabronione jest umożliwianie innym osobom pracy na koncie innego użytkownika.
10. Zabrania się pracy wielu użytkowników na wspólnym koncie.

11. Użytkownik (np. komputera stacjonarnego, laptopa, dysku sieciowego, programów w których użytkownik pracuje, poczty elektronicznej) rozpoczyna pracę z użyciem identyfikatora i hasła.
12. Użytkownik jest zobowiązany do powiadomienia nauczyciela o próbach logowania się do systemu osoby nieupoważnionej, jeśli system to sygnalizuje.
13. Po zakończeniu pracy, użytkownik zobowiązany jest:
    a) wylogować się z systemu informatycznego, a następnie wyłączyć sprzęt komputerowy,
    b) zabezpieczyć stanowisko pracy, w szczególności wszelką dokumentację oraz nośniki magnetyczne i optyczne, na których znajdują się dane osobowe.
18. Hasła powinny składać się z 8 znaków.
19. Hasła powinny zawierać duże litery + małe litery + cyfry + znaki specjalne.
20. Hasła nie mogą być łatwe do odgadnięcia. Nie powinny być powszechnie używanymi słowami. W szczególności nie należy jako haseł wykorzystywać: dat, imion i nazwisk osób bliskich, imion zwierząt, popularnych dat, popularnych słów, typowych zestawów: 123456, qwerty, itd.
21. Hasła nie powinny być ujawnianie innym osobom. Nie należy zapisywać haseł na kartkach i w notesach, nie naklejać na monitorze komputera, nie trzymać pod klawiaturą lub w szufladzie.
22. W przypadku ujawnienia hasła – należy natychmiast je zmienić.
23. Hasła powinny być zmieniane co 30 dni.
24. Jeżeli system nie wymusza zmiany haseł, użytkownik zobowiązany jest do samodzielnej zmiany hasła.
25. Użytkownik systemu w trakcie pracy w aplikacji może zmienić swoje hasło.
26. Użytkownik zobowiązuje się do zachowania hasła w poufności, nawet po utracie przez nie ważności.
27. Zabrania się stosowania tego samego hasła jako zabezpieczenia w dostępie do różnych systemów.
28. Nie powinno się też stosować haseł, w których któryś z członów stanowi imię, nazwę lub numer miesiąca lub inny możliwy do odgadnięcia klucz.

**Bezpieczne korzystanie z Internetu**

29. W trakcie nauczania zdalnego nauczyciel powinien stale przypominać uczniom o zasadach bezpiecznego korzystania z sieci, szczególną uwagę, zwracając na uczniów niepełnosprawnych.
30. Zabrania się zgrywania na dysk twardy komputera służbowego oraz uruchamia jakichkolwiek programów nielegalnych oraz plików pobranych z niewiadomego źródła.
31. Zabrania się wchodzenia na strony, na których prezentowane są informacje o charakterze przestępczym, hackerskim, pornograficznym, lub innym zakazanym przez

prawo (na większości stron tego typu jest zainstalowane szkodliwe oprogramowanie infekujące w sposób automatyczny system operacyjny komputera szkodliwym oprogramowaniem).

32. Nie należy w opcjach przeglądarki internetowej włączać opcji autouzupełniania formularzy i zapamiętywania haseł.
33. W przypadku korzystania z szyfrowanego połączenia przez przeglądarkę, należy zwracać uwagę na pojawienie się odpowiedniej ikonki (kłódka) oraz adresu www rozpoczynającego się frazą "https:". Dla pewności należy „kliknąć" na ikonkę kłódki i sprawdzić, czy właścicielem certyfikatu jest wiarygodny właściciel.
34. Należy zachować szczególną ostrożność w przypadku podejrzanego żądania lub prośby zalogowania się na stronę (np. na stronę banku, portalu społecznościowego, e-sklepu, poczty mailowej) lub podania naszych loginów i haseł, PIN-ów, numerów kart płatniczych przez Internet. Szczególnie tyczy się to żądania podania takich informacji przez rzekomy bank.

**Zasady korzystania z poczty elektronicznej**

35. W przypadku zdalnego nauczania nauczyciele oraz pracownicy szkoły powinni korzystać ze służbowej poczty mailowej.
36. W przypadku przesyłania danych osobowych należy wysyłać pliki zaszyfrowane/spakowane (np. programem 7 zip, winzipem, winrarem) i zahasłowane, gdzie hasło powinno być przesłane do odbiorcy telefonicznie lub SMS.
37. W przypadku zabezpieczenia plików hasłem, obowiązuje minimum 8 znaków: duże i małe litery i cyfry i znaki specjalne, a hasło należy przesłać odrębnym mailem lub inną metodą, np. telefonicznie lub SMS-em.
38. Użytkownicy powinni zwracać szczególną uwagę na poprawność adresu odbiorcy dokumentu.
39. Zaleca się, aby użytkownik podczas przesyłania danych osobowych mailem zawarł w treści prośbę o potwierdzenie otrzymania i zapoznania się z informacją przez adresata.
40. WAŻNE: Nie otwierać załączników od nieznanych nadawców typu .zip, .xlsm, .pdf, .exe w mailach!!!!! Są to zwykle „wirusy", które infekują komputer oraz często pozostałe komputery w sieci. WYSOKIE RYZYKO UTRATY BEZPOWROTNEJ UTRATY DANYCH.
41. WAŻNE: Nie wolno „klikać" na hiperlinki w mailach, gdyż mogą to być hiperlinki do stron z „wirusami". Użytkownik „klikając" na taki hiperlink infekuje komputer oraz inne komputery w sieci.
42. Podczas wysyłania maili do wielu adresatów jednocześnie, należy użyć metody „Ukryte do wiadomości – UDW". Zabronione jest rozsyłanie maili do wielu adresatów z użyciem opcji „Do wiadomości"!
43. Użytkownicy powinni okresowo kasować niepotrzebne maile.
44. Mail służbowy jest przeznaczony wyłącznie do wykonywania obowiązków służbowych.

45. Przy korzystaniu z maila, użytkownicy mają obowiązek przestrzegać prawa własności przemysłowej i prawa autorskiego.
46. Użytkownicy nie mają prawa korzystać z maila w celu rozpowszechniania treści o charakterze obraźliwym, niemoralnym lub niestosownym wobec powszechnie obowiązujących zasad postępowania.

Z up. Dyrektora
Wicedyrektor
*mgr inż. Anna Balcerowska*