Pieczęć administratora

PODSTAWOWE ZASADY PRZETWARZANIA I OCHRONY DANYCH OSOBOWYCH U ADMINISTRATORA

1. Pomieszczenia i szafki, w których przetwarzane są dane osobowe, powinny być zamykane na klucz.
2. W przypadku nieobecności pracownika w pomieszczeniu, w którym przetwarzane są dane osobowe, pomieszczenie należy zamknąć na klucz, w celu uniemożliwienia dostępu do pomieszczenia osobom nieuprawnionym.
3. Sprzątanie pomieszczeń, w których przetwarzane są dane osobowe, powinno odbywać się w godzinach pracy i pod nadzorem osoby upoważnionej do przetwarzania tych danych. W przypadku, w którym sprzątanie odbywałoby się poza godzinami pracy, dostęp do danych osobowych powinien zostać uniemożliwiony poprzez ukrycie tych danych w szafach i zamknięcie ich na klucz.
4. Niedopuszczalne jest pozostawianie klucza w zamkach drzwi i szaf w przypadku choćby czasowej nieobecności pracownika w pomieszczeniu, w którym przetwarzane są dane osobowe.
5. Zaleca się prowadzenie rejestru wydawanych kluczy do pomieszczeń i szaf dla uprawnionych pracowników. Klucze te powinny być przechowywane w odpowiednio zabezpieczonej w tym celu szafie (pojemniku, skrzynce, gablocie). Niedopuszczalne jest wynoszenie przez pracowników kluczy poza budynek Administratora, a także ich samowolne dorabianie.
6. Monitory znajdujące się w pomieszczeniach, w których przetwarzane są dane osobowe, powinny być ustawione w sposób uniemożliwiający odczytanie zawartości ekranu osobom nieupoważnionym, bądź przed takim odczytaniem zabezpieczone stosownymi fizycznymi środkami zabezpieczeń (np. filtry prywatyzujące, folie na oknach, rolety). Komputery, laptopy oraz inne urządzenia elektroniczne powinny być zabezpieczone poprzez zastosowanie wygaszacza ekranu włączającego się automatycznie po określonym przez Administratora czasie oraz automatycznego blokowania dostępu w przypadku bezczynności użytkownika, aktywowanego za pomocą loginu oraz hasła. Opuszczając stanowisko pracy należy blokować komputer poprzez jednoczesne naciśnięcie klawiszy CTRL+ALT+DEL oraz wybranie opcji „ZABLOKUJ KOMPUTER" (polityka czystego ekranu).
7. Niedopuszczalne jest pozostawianie na biurkach oraz w innych miejscach dokumentów zawierających dane osobowe, niezależnie od nośnika na jakim są one zapisane, w sposób umożliwiający ich odczytanie i dostęp do nich osobom nieuprawnionym (polityka czystego biurka).
8. Dostęp do systemów informatycznych powinien być zabezpieczony za pomocą nadania użytkownikom indywidualnych loginów i haseł. Hasło powinno składać się z przynajmniej 8 znaków, w tym wielkich i małych liter, znaków specjalnych i cyfr. Hasło musi być zmieniane w określonych przez Administratora okresach, nie rzadziej jednak niż raz na pół roku. W tym celu zalecane jest wprowadzenie rozwiązań wymuszających okresową zmianę haseł, jednak w przypadku braku takiego rozwiązania, użytkownik zobowiązany jest do samodzielnego dokonywania okresowych zmian haseł.
9. Niedopuszczalne jest zapisywanie nadanych haseł i umieszczanie ich w ogólnodostępnych miejscach, jak również ujawnianie ich osobom nieupoważnionym.

Wersja 1.0 maj 2018

10. Uprawnienia w systemach informatycznych powinny być przydzielane wyłącznie w zakresie niezbędnym do wykonywania praw i obowiązków na danym stanowisku.
11. Sprzęt komputerowy (np. komputery, stacje robocze, laptopy, tablety) oraz nośniki danych (np. dyski, pendrive'y, płyty CD) nie powinny być wynoszone poza budynek Administratora. W przypadku umożliwienia wynoszenia wskazanego sprzętu/nośników, osobom uprawnionym do tego powinny zostać wydane przez Administratora stosowne upoważnienia, a same urządzenia/nośniki powinny zostać stosownie zabezpieczone, np. przez zaszyfrowanie. Zaleca się prowadzenie rejestru urządzeń elektronicznych oraz nośników danych, a także osób upoważnionych do ich wynoszenia poza budynek Administratora.
12. Służbowe telefony komórkowe powinny zostać stosownie zabezpieczone, np. przez zaszyfrowanie. Zaleca się prowadzenie rejestru służbowych telefonów komórkowych.
13. Zaleca się stosowanie szyfrowania dysków, plików, transmisji oraz nośników zawierających dane osobowe, a także dokumentów przesyłanych za pomocą skrzynki e-mail.
14. W przypadku podłączenia urządzeń lub nośników zewnętrznych, konieczne jest ich uprzednie sprawdzenie pod kątem potencjalnych zagrożeń, w tym wirusami, końmi trojańskimi, robakami, itp. Nie wolno korzystać z nośników z nieznanego źródła (np. znalezionych na terenie placówki).
15. Podczas odbierania poczty elektronicznej (e-mail) należy zwracać szczególną uwagę na załączniki pochodzące od nieznanych nadawców, mogą bowiem zawierać złośliwe oprogramowanie. W razie wątpliwości należy wstrzymać się z otwieraniem załącznika i skontaktować z osobą odpowiedzialną za obsługę informatyczną podmiotu. Zabrania się samodzielnego instalowania jakiegokolwiek oprogramowania oraz przechowywania na służbowych komputerach materiałów prywatnych.
16. Urządzenia służące do wydruku oraz kopiowania i skanowania nie powinny znajdować się w ogólnodostępnym miejscu, a jeżeli się znajdują, drukowanie/kopiowanie/skanowanie powinno odbywać się pod ścisłym nadzorem osoby upoważnionej do przetwarzania określonych danych osobowych. Przed wysłaniem dokumentu do wydruku należy każdorazowo upewnić się czy prawidłowo wybrano urządzenie drukujące. Żadne dokumenty nie powinny pozostawać bez nadzoru w urządzeniach typu drukarka, ksero, scaner.
17. Niedozwolone jest kopiowanie, skanowanie i czasowe zatrzymywanie dowodów tożsamości, chyba że takie uprawnienie lub obowiązek wprost wynika z przepisu prawa.
18. Nie wolno wyrzucać do kosza jakichkolwiek dokumentów zawierających dane osobowe. Wszelkie dokumenty przeznaczone do zniszczenia, powinny być niszczone w sposób uniemożliwiający ich odczytanie.
19. W salach konferencyjnych/pokojach spotkań nie powinno się pozostawiać żadnych dokumentów, nośników danych, plików na ogólnodostępnych komputerach czy informacji na tablicach.
20. Niedopuszczalne jest umieszczanie w listach obecności informacji o powodach nieobecności pracowników, w szczególności o powodach zdrowotnych.
21. Listy obecności i inne dokumenty pracownicze, a także dotyczące osób trzecich, nie powinny być pozostawiane w ogólnodostępnych miejscach i bez nadzoru.
22. Zaleca się prowadzenie rejestru interesantów, w celu zabezpieczenia rozliczalności w przypadku utraty danych osobowych.
23. Zaleca się ustalenie „strefy bezpieczeństwa" w pomieszczeniach, w których dokonywana jest obsługa/rejestracja interesantów/klientów/pacjentów w taki sposób, aby uniemożliwić osobom nieupoważnionym pozyskanie informacji na temat danych osoby obsługiwanej. Dane osobowe zawarte w dowodzie tożsamości nie mogą być odczytywane na głos.
24. Zaleca się nadawanie interesantom/klientom/pacjentom numerów, w celu uniknięcia konieczności wywoływania ich przy wykorzystaniu imienia i nazwiska; gdy jest to niemożliwe, zaleca się wywoływanie osób obsługiwanych przy użyciu samego imienia lub innego identyfikatora

określonego przez Administratora. Zabrania się wywoływania osób obsługiwanych przez podawanie ich nazwisk.

25. Należy niezwłocznie zgłaszać Administratorowi wszelkie podejrzenia dotyczące naruszenia powyższych zasad.

Zatwierdzam i nakazuję stosować.

DYREKTOR SZKOŁY

3.09.2018 mgr Anna Kanafa

data i podpis Administratora