**REGULAMIN OCHRONY DANYCH OSOBOWYCH I KORZYSTANIA ZE SPRZĘTU IT**

**W SZKOLE PODSTAWOWEJ W SŁAWIANOWIE.**

*Podstawa prawna: Ustawa z dnia 29 sierpnia 1997r. o ochronie danych osobowych (Dz.U. z 2016r., poz. 922); rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z 27 kwietnia 2016r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46 WE (ogólne rozporządzenie o ochronie danych).*

**§ 1**. **Zasady bezpiecznego użytkowania sprzętu IT:**

1. **Zabronione** **jest wykorzystywanie przez pracownika komputera służbowego do celów prywatnych.** W szczególności zabronione jest instalowanie i wykorzystywanie jakiegokolwiek oprogramowania bez wiedzy i udziału osób odpowiedzialnych za tego rodzaju czynności.
2. Użytkownik odpowiada za zabezpieczenie przed zniszczeniem, uszkodzeniem oraz utratą sprzętu IT (komputery, skanery, smartfony, służbowe tablety lub laptopy).
3. Samowolne instalowanie, demontaż oraz podłączanie dodatkowych urządzeń np. twardych dysków lub innych nośników pamięci jest **zabronione.**
4. Użytkownik jest zobowiązany zgłosić zagubienie, utratę lub zniszczenie powierzonego mu sprzętu IT.
5. Użytkownik jest zobowiązany do usuwania plików z nośników/dysków do których mają dostęp inni użytkownicy nieupoważnieni do dostępu do takich plików, np. podczas współużytkowania komputerów.
6. Użytkownik jest zobowiązany do przekazania informatykowi nośników przeznaczonych do zniszczenia.
7. Na komputerach wykorzystywanych przez nauczycieli w pracowniach lekcyjnych tworzone są następujące konta:
8. Administrator – zabezpieczone hasłem znanym jedynie dla administratora systemu,
9. Nauczyciel – zabezpieczone hasłem jednakowym na wszystkich komputerach. Konto to służy wyłącznie do prowadzenia bieżącej lekcji. Wszystkie dokumenty użyte do przeprowadzenia lekcji muszą być usunięte po jej zakończeniu.

**§ 2.** **Zarządzanie uprawnieniami – procedura rozpoczęcia, zawieszenia i zakończenia pracy:**

1. Każdy użytkownik komputera stacjonarnego, laptopa, programów i systemów operacyjnych zobowiązany jest do pracy na własnym koncie. Zabronione jest udostępnianie konta innemu użytkownikowi.
2. Użytkownik nie może zmieniać swoich uprawnień, np. zostać administratorem na swoim komputerze.
3. Użytkownik komputerów oraz programów rozpoczyna i kończy pracę logowaniem i wylogowaniem się .
4. Użytkownik jest zobowiązany do uniemożliwienia osobom niepowołanym wglądu do danych wyświetlanych na monitorach – tzw. Polityka czystego ekranu.
5. Użytkownik przed czasowym odejściem od komputera musi włączyć wygaszacz ekranu lub wylogować się z systemu bądź programu.
6. Zabrania się uruchamiania jakiejkolwiek aplikacji lub programu na prośbę innej osoby, o ile nie została ona zweryfikowana. Dotyczy to zwłaszcza programów przesłanych za pomocą poczty elektronicznej lub wskazana w formie załącznika internetowego.
7. Po zakończeniu pracy, użytkownik zobowiązany jest wylogować się z systemu informatycznego oraz zabezpieczyć nośniki elektroniczne, magnetyczne i optyczne na których znajdują się dane osobowe.

**§ 3**. **Polityka haseł:**

1. Hasła powinny się składać z co najmniej 8 znaków.
2. Hasła powinny zawierać duże litery + małe litery + cyfry (lub znaki specjalne).
3. Hasła nie mogą być łatwe do odgadnięcia. Nie powinny być powszechnie używanymi słowami.
4. Hasła nie powinny być ujawniane innym osobom. Nie należy zapisywać haseł na kartkach i w notesach, nie naklejać na monitorze komputera, nie trzymać pod klawiaturą lub w szufladzie.
5. W przypadku ujawnienia hasła – należy go natychmiast zmienić.
6. Hasła muszą być zmieniane co 90 dni.
7. Jeżeli system nie wymusza zmiany haseł, użytkownik zobowiązany jest do samodzielnej zmiany hasła.

**§ 4. Zabezpieczenie dokumentacji papierowej z danymi osobowymi:**

1. Pracownicy zobowiązani są do niszczenia dokumentów i wydruków w niszczarkach.
2. Zabrania się pozostawiania dokumentów w miejscach dostępnych dla osób postronnych.
3. Zabrania się wyrzucania niszczonych dokumentów na śmietnik.

**§ 5**. **Zasady wynoszenia nośników z danymi poza szkołę:**

1. Użytkownicy **nie mogą** wynosić poza miejsce pracy laptopów, służbowych tabletów, niezaszyfrowanych nośników z danymi osobowymi (np. przenośnych dysków twardych, pen-drive, płyt CD, DVD oraz pamięci typu Flash) bez zgody dyrektora szkoły.
2. Dane osobowe wynoszone poza szkołę muszą być zaszyfrowane (szyfrowane dyski przenośne, zahasłowane pliki, zabezpieczone smartfony).

**§ 6.** **Zasady korzystania z Internetu:**

1. Użytkownik zobowiązany jest do korzystania z Internetu **wyłącznie** w celach służbowych.
2. Zabrania się zgrywania na dysk twardy komputera oraz uruchamianie jakichkolwiek programów nielegalnych oraz plików pobranych z niewiadomego źródła. Pliki takie powinny być ściągane tylko za zgodą osoby upoważnionej do administrowania infrastrukturą IT i tylko w uzasadnionych przypadkach.
3. Użytkownik ponosi odpowiedzialność za szkody spowodowane przez oprogramowanie instalowane z Internetu.
4. Zabrania się wchodzenia na strony, na których prezentowane są informacje o charakterze przestępczym, hackerskim.
5. Nie należy w opcjach przeglądarki internetowej włączać opcji autouzupełniania formularzy i zapamiętywania haseł.

**§ 7. Zasady Korzystania z poczty elektronicznej:**

1. Pliki z danymi osobowymi w Wordzie , Excelu, w PDF lub spakowane (7zip) przed wysłaniem ich do osób trzecich powinny być zahasłowane a hasło powinno być przesłane do odbiorcy telefonicznie lub SMS.
2. Użytkownicy powinni zwracać szczególną uwagę na poprawność adresu odbiorcy dokumentu.
3. **WAŻNE:** **Nie otwierać załączników (zip, rar, xlsm, pdf, exe) w mailach od nieznanego adresata!!! Są to zwykle „wirusy”, które infekują komputer oraz często pozostałe komputery w sieci.** WYSOKIE RYZYKO UTRATY BEZPOWROTNIE DANYCH.
4. Należy zgłaszać informatyki przypadki podejrzanych emaili.
5. Podczas wysyłania maili do wielu adresatów jednocześnie, należy użyć metody **„Ukryte wiadomości UDW”**. Zabronione jest rozsyłanie maili do wielu adresatów z użyciem opcji **„Do wiadomości”!**
6. Użytkownicy powinni okresowo kasować niepotrzebne maile.
7. **Zakazuje się** wysyłania korespondencji służbowej na prywatne skrzynki pocztowe pracowników lub innych osób.
8. Użytkownik bez zgody Pracodawcy nie ma prawa wysyłać wiadomości zawierających dane osobowe dotyczące Pracodawcy, współpracowników i uczniów.

**§ 8. Postępowanie w przypadku naruszenia danych osobowych:**

1. Każda osoba upoważniona do przetwarzania danych osobowych zobowiązana jest do powiadomienia Pracodawcy w przypadku stwierdzenia lub podejrzenia naruszenia ochrony danych osobowych.
2. Do sytuacji wymagających powiadomienia, należą:
3. niewłaściwe zabezpieczenie fizyczne pomieszczeń, urządzeń i dokumentów,
4. niewłaściwe zabezpieczenie sprzętu IT, oprogramowania przed wyciekiem, kradzieżą i utratą danych osobowych,
5. nieprzestrzeganie zasad ochrony danych osobowych przez pracowników (np. niestosowanie zasady czystego biurka/ekranu, ochrony haseł, niezamykanie pomieszczeń, szaf, biurek).
6. Do incydentów wymagających powiadomienia, należą:
7. zdarzenia losowe zewnętrzne (pożar obiektu/pomieszczenia, zalanie wodą, utrata zasilania, utrata łączności),
8. zdarzenia losowe wewnętrzne (awaria serwera, komputerów, twardych dysków, oprogramowania, utrata/zagubienie danych),
9. umyślne incydenty (włamanie do systemu informatycznego lub pomieszczeń, kradzież danych/sprzętu, wyciek informacji, ujawnienie danych osobom nieupoważnionym, świadome zniszczenie dokumentów, działanie wirusów i inne szkodliwe oprogramowania).
10. Typowe przykłady incydentów wymagających reakcji:
11. ślady w drzwiach, oknach i szafach wskazują na próbę włamania,
12. dokumentacja jest niszczona bez użycia niszczarki,
13. fizyczna obecność w budynku lub pomieszczeniach osób zachowujących się podejrzanie,
14. otwarte drzwi do pomieszczeń, szaf, gdzie przechowywane są dane osobowe,
15. ustawienie monitora pozwala na wgląd osób postronnych w dane osobowe,
16. wynoszenie danych osobowych w wersji papierowej i elektronicznej poza miejsce pracy bez zgody pracodawcy,
17. udostępnianie danych osobowych osobom nieupoważniony w formie elektronicznej, papierowej lub ustnej,
18. telefoniczne próby wyłudzenia danych osobowych,
19. kradzież, zagubienie laptopa lub CD/DVD, twardych dysków, pen-drive z danymi osobowymi,
20. maile zachęcające do ujawnienia identyfikatora i/lub hasła,
21. pojawienie się wirusa komputerowego lub niestandardowe zachowanie komputerów,
22. hasła do systemów przyklejone są w pobliżu komputera.

**§ 9. Obowiązek zachowania poufności i ochrony danych osobowych:**

1. Każda z osób dopuszczona do przetwarzania danych osobowych jest zobowiązana do :
2. Przetwarzania danych osobowych wyłącznie w celu i zakresie powierzonych obowiązków,
3. Zachowania w tajemnicy danych osobowych do których ma dostęp,
4. Niewykorzystywania danych osobowych w celach niezgodnych z zakresem i celem powierzonych jej zadań i obowiązków,
5. Zachowania w tajemnicy sposobów zabezpieczenia danych osobowych.
6. Zabrania się przekazywania bezpośrednio lub przez telefon danych osobowych osobom nieupoważnionym lub osobom, których tożsamość nie może być zweryfikowana lub osobom podszywającym się pod kogoś innego.
7. Zabrania się przekazywania lub ujawniania danych osobom lub instytucjom, które nie mogą wykazać się jasną podstawą prawną do dostępu do takich danych.
8. Każda z osób dopuszczonych do przetwarzania danych osobowych jest zobowiązana zabezpieczyć dane osobowe przed przypadkowym lub niezgodnym z prawem zniszczeniem, utratą, modyfikacją, nieuprawnionym dostępem do danych osobowych oraz przetwarzaniem.

**§ 10. Postępowanie dyscyplinarne**

1. Przypadki nieuzasadnionego zaniechania obowiązków wynikających z niniejszego dokumentu potraktowane będą jako ciężkie naruszenie obowiązków pracowniczych lub naruszenie zasad współpracy.
2. Postępowanie sprzeczne z powyższymi zobowiązaniami, może też być uznane przez Pracodawcę za naruszenie przepisów karnych zawartych w ogólnym Rozporządzeniu o Ochronie Danych Osobowych UE z dnia 27 kwietnia 2016r.

25.05.2018r.

Opracował:

Inspektor ochrony danych osobowych

Emilia Hudowicz