**REGULAMIN**

**„ZASADY OCHRONY DANYCH OSOBOWYCH”**

**W**

**PRZEDSZKOLU NR 2 W KOLUSZKACH**

1. Każdy pracownik przetwarza dane osobowe wyłącznie w związku

z wykonywaniem zadań służbowych.

1. Udostępnianie danych osobom trzecim jest zabronione.
2. Pracownik jest obowiązany logować się do systemu za pomocą własnego loginu oraz hasła dostępu. Udzielanie informacji na temat loginu innym osobom jest zabronione.
3. Pracownik ma prawo korzystać z Internetu wyłącznie w celu wykonywania obowiązków służbowych.
4. Opuszczając czasowo stanowisko pracy pracownik ma obowiązek zablokować komputer poprzez wylogowanie się z programu oraz dokonać blokady systemu operacyjnego.
5. Kończąc pracę pracownik pozostaje przy stanowisku komputerowym do czasu całkowitego wyłączenia się komputera.
6. Zabronione jest korzystanie z prywatnych nośników informacji (np. dysk zewnętrzny, PenDrive).
7. Bez potrzeby nie należy tworzyć plików komputerowych zawierających dane osobowe. Pliki z danymi po ustaniu przydatności należy usunąć.
8. Bez potrzeby nie należy kopiować ani drukować dokumentów zawierających dane osobowe – zmniejsza się wówczas ryzyko udostępnienia danych osobowym nieupoważnionym.
9. Wszelkie dokumenty zawierające dane osobowe należy niszczyć za pomocą niszczarek dokumentów.
10. Za bezpieczeństwo dokumentów i wydruków zawierających dane osobowe odpowiedzialne są osoby upoważnione (użytkownicy) oraz kierownicy właściwych jednostek organizacyjnych.
11. Dokumenty i wydruki zawierające dane osobowe przechowuje się

w pomieszczeniach zabezpieczonych fizycznie przed dostępem osób nieupoważnionych.

1. Użytkownicy są zobowiązani do stosowania „polityki czystego biurka”. Polega ona na zabezpieczaniu dokumentów np. w szafach, biurkach, pomieszczeniach przed kradzieżą lub wglądem osób nieupoważnionych.
2. Użytkownicy zobowiązani są do przewożenia dokumentów w sposób zapobiegający ich kradzieży, zagubieniu lub utracie.
3. Użytkownicy zobowiązani są do niszczenia dokumentów i tymczasowych wydruków w niszczarkach niezwłocznie po ustaniu celu ich przetwarzania.

**Skrócona instrukcja postępowania w przypadku naruszenia ochrony danych osobowych**

1. Użytkownik zobowiązany jest do powiadomienia Inspektora Ochrony Danych – p. K. Sybilską (dane na niebieskim pasku) w przypadku stwierdzenia lub podejrzenia naruszenia ochrony danych osobowych
2. Typowe sytuacje, gdy użytkownik powinien powiadomić IOD:
	1. ślady na drzwiach, oknach i szafach wskazują na próbę włamania;
	2. dokumentacja jest niszczona bez użycia niszczarki;
	3. fizyczna obecność w budynku lub pomieszczeniach osób zachowujących się podejrzanie;
	4. otwarte drzwi do pomieszczeń, szaf, gdzie przechowywane są dane osobowe;
	5. ustawienie monitorów pozwala osobom postronnym na wgląd

w dane osobowe wyświetlane na monitorze;

* 1. wynoszenie danych osobowych w wersji papierowej i elektronicznej poza firmę bez upoważnienia IOD;
	2. udostępnienie danych osobowych osobom nieupoważnionym

w formie papierowej, elektronicznej i ustnej;

* 1. telefoniczne próby wyłudzenia danych osobowych;
	2. kradzież komputerów lub CD, twardych dysków, Pen-drive z danymi osobowymi;
	3. maile zachęcające do ujawnienia identyfikatora i/lub hasła;
	4. pojawienie się wirusa komputerowego lub niestandardowe zachowanie komputerów;
	5. hasła do systemów przechowywane są w pobliżu komputera.