

Ostrzeżenia dotyczące bezpieczeństwa dla programów biurowych

(Zgodnie z Rozporządzeniem Parlamentu Europejskiego i Rady (UE) 2023/988 w sprawie ogólnego bezpieczeństwa produktów – GPSR)

Ważne! Choć oprogramowanie biurowe jest narzędziem cyfrowym, jego długotrwałe i niewłaściwe użytkowanie wiąże się z ryzykiem zdrowotnym (ergonomia) oraz zagrożeniami dla bezpieczeństwa danych (cyberbezpieczeństwo).

1. Ergonomia i zdrowie użytkownika

- **Ryzyko chorób układu mięśniowo-szkieletowego (Krytyczne):** Długotrwała praca z programami biurowymi w niewłaściwej pozycji może prowadzić do zespołu cieśni nadgarstka, bólów kręgosłupa oraz zwyrodnień stawów. Należy stosować zasady ergonomii: monitor na wysokości oczu, stopy płasko na podłodze, wsparcie lędźwiowe.
- **Ochrona wzroku:** Intensywne wpatrywanie się w arkusze kalkulacyjne lub długie teksty powoduje cyfrowe zmęczenie wzroku (zespół CVS). Stosuj zasadę 20-20-20: co 20 minut spójrz na obiekt oddalony o ok. 6 metrów przez 20 sekund.
- **Przerwy w pracy:** Praca z oprogramowaniem biurowym wymaga regularnych przerw (minimum 5 minut po każdej godzinie pracy), aby uniknąć przeciążenia statycznego mięśni i zmęczenia poznawczego.

2. Cyberbezpieczeństwo i ochrona danych

- **Ryzyko złośliwego oprogramowania (Krytyczne):** Pliki pakietów biurowych mogą zawierać szkodliwe skrypty (makra). Nigdy nie otwieraj plików z nieznanych źródeł i nie włączaj makr w dokumentach przesłanych przez e-mail, jeśli nie masz pewności co do ich pochodzenia. Może to doprowadzić do kradzieży danych lub zainfekowania komputera wirusem typu ransomware.

- **Prywatność danych i metadane:** Pamiętaj, że dokumenty biurowe przechowują metadane (np. autora, czas edycji, historię zmian). Przed udostępnieniem pliku osobom trzecim, użyj funkcji „inspekcji dokumentu”, aby usunąć wrażliwe informacje osobiste.
- **Hasła i szyfrowanie:** Jeśli dokument zawiera dane poufne (finanse, dane osobowe), zawsze stosuj funkcję szyfrowania hasłem dostępną w programie. Unikaj przesyłania niezaszyfrowanych arkuszy z danymi wrażliwymi przez niezabezpieczone kanały komunikacji.

3. Bezpieczeństwo techniczne i ciągłość pracy

- **Utrata danych:** Błędy oprogramowania, awarie zasilania lub błędy systemu mogą doprowadzić do utraty niezapisanych wyników pracy. Skonfiguruj funkcję „Autozapisu” i regularnie twórz kopie zapasowe (backup) ważnych plików.
- **Aktualizacje oprogramowania:** Korzystanie z nieaktualnych wersji programów biurowych naraża system na ataki hakerskie wykorzystujące znane luki w zabezpieczeniach. Zawsze instaluj najnowsze poprawki bezpieczeństwa udostępniane przez producenta.
- **Legalność oprogramowania:** Używaj wyłącznie legalnych kopii programów. „Pęknięte” (pirackie) wersje oprogramowania biurowego często zawierają wbudowane trojany, które monitorują aktywność i wykradają hasła.

4. Zarządzanie dostępem

- **Uwierzytelnianie dwuskładnikowe (2FA):** Jeśli Twoje programy biurowe są powiązane z kontem w chmurze (np. Microsoft 365, Google Workspace), zabezpiecz dostęp do nich za pomocą 2FA. Przejęcie konta daje napastnikowi dostęp do wszystkich Twoich dokumentów.

- **Wygasanie licencji:** Monitoruj okres ważności subskrypcji. Wygaśnięcie licencji może zablokować możliwość edycji ważnych dokumentów w krytycznym momencie.

5. Utylizacja nośników i danych

- **Trwałe usuwanie danych:** Przed sprzedażą lub wyrzuceniem nośnika (komputera, pendrive'a), na którym znajdowały się dokumenty biurowe, upewnij się, że dane zostały trwale nadpisane, a nie tylko przeniesione do kosza.
- **Recykling sprzętu:** Stare płyty instalacyjne CD/DVD oraz uszkodzone nośniki USB traktuj jako elektroodpady i oddaj do punktu zbiórki ZSEE.