

Instrukcja Bezpieczeństwa - Programy Biurowe

Zgodna z wymogami Rozporządzenia (UE) 2023/988 - GPSR

Ważne: Przed rozpoczęciem instalacji i użytkowania programów biurowych, prosimy o dokładne zapoznanie się z poniższymi informacjami dotyczącymi bezpieczeństwa. Przestrzeganie tych zasad pomoże chronić Twoje dane, urządzenie oraz prywatność.

1. Ogólne Zasady Bezpieczeństwa

- **Cel Instrukcji:** Niniejsza instrukcja ma na celu poinformowanie użytkowników o potencjalnych ryzykach związanych z użytkowaniem programów biurowych oraz wskazanie środków ostrożności minimalizujących te ryzyka.
- **Odpowiedzialność Użytkownika:** Bezpieczne korzystanie z oprogramowania zależy również od świadomości i działań użytkownika.

2. Instalacja i Aktualizacje

- **Legalne Źródła:** Pobieraj i instaluj programy biurowe wyłącznie z oficjalnych i zaufanych źródeł (np. strona internetowa producenta, autoryzowani dystrybutorzy, oficjalne sklepy z aplikacjami). Unikaj pobierania oprogramowania z nieznanych stron, P2P lub linków w podejrzanych wiadomościach.
- **Regularne Aktualizacje:** Utrzymuj oprogramowanie biurowe oraz system operacyjny swojego urządzenia w najnowszej wersji. Aktualizacje często zawierają krytyczne poprawki bezpieczeństwa, które chronią przed nowymi zagrożeniami (np. wirusami, złośliwym oprogramowaniem). Włącz automatyczne aktualizacje, jeśli to możliwe.
- **Unikaj Modyfikacji:** Nie instaluj nieoficjalnych dodatków, "cracków" ani modyfikacji oprogramowania, ponieważ mogą one zawierać ukryte złośliwe funkcje lub naruszać stabilność i bezpieczeństwo systemu.

3. Bezpieczeństwo Danych i Prywatność

- **Kopie Zapasowe (Backup):** Regularnie twórz kopie zapasowe ważnych plików i dokumentów tworzonych lub edytowanych za pomocą programów biurowych. Przechowuj kopie w bezpiecznym miejscu, najlepiej oddzielnie od głównego urządzenia (np. na zewnętrznym dysku, w bezpiecznej chmurze). Testuj możliwość odtworzenia danych z kopii zapasowej.
- **Ochrona Hasłem:** Jeśli oprogramowanie oferuje możliwość zabezpieczenia plików hasłem, korzystaj z tej funkcji dla dokumentów zawierających dane wrażliwe lub poufne. Używaj silnych, unikalnych haseł.

- **Ostrożność przy Otwieraniu Plików:** Bądź szczególnie ostrożny podczas otwierania plików (np. .docx, .xlsx, .pdf, .zip) otrzymanych z nieznanych lub nieoczekiwanych źródeł, zwłaszcza jako załączniki w e-mailach. Mogą one zawierać złośliwe oprogramowanie (malware, ransomware).
- **Makra:** Wyłączaj automatyczne uruchamianie makr w programach biurowych. Uruchamiaj makra tylko wtedy, gdy jesteś absolutnie pewien ich pochodzenia i bezpieczeństwa. Złośliwe makra są częstym wektorem ataków.
- **Phishing i Oszustwa:** Uważaj na próby wyłudzenia informacji (phishing) za pośrednictwem wiadomości e-mail lub fałszywych powiadomień, które mogą wydawać się pochodzić od dostawcy oprogramowania lub współpracowników. Nie klikaj podejrzanych linków ani nie podawaj danych logowania czy danych osobowych w odpowiedzi na takie wiadomości.
- **Ustawienia Prywatności:** Zapoznaj się z ustawieniami prywatności oprogramowania, szczególnie jeśli korzysta ono z funkcji chmurowych, udostępniania lub telemetrii. Dostosuj je do swoich preferencji i potrzeb w zakresie ochrony danych.
- **Udostępnianie Plików:** Bądź świadomy, komu i w jaki sposób udostępniasz pliki stworzone w programach biurowych, zwłaszcza jeśli zawierają dane osobowe lub poufne informacje. Korzystaj z bezpiecznych metod udostępniania.

4. Bezpieczne Użytkowanie

- **Oprogramowanie Antywirusowe:** Upewnij się, że na Twoim urządzeniu jest zainstalowane i aktywne renomowane, aktualne oprogramowanie antywirusowe/antymalware. Regularnie skanuj system.
- **Regularne Zapisywanie Pracy:** Często zapisuj postępy swojej pracy, aby zminimalizować ryzyko utraty danych w przypadku nieoczekiwanej awarii oprogramowania, systemu operacyjnego lub zasilania.
- **Bezpieczne Sieci:** Unikaj pracy z wrażliwymi danymi w programach biurowych podczas połączenia z niezaufanymi lub publicznymi sieciami Wi-Fi.
- **Ergonomia (Uwaga Dodatkowa):** Długotrwała praca przy komputerze z użyciem programów biurowych może wpływać na zdrowie. Dbaj o ergonomiczne ustawienie stanowiska pracy, prawidłową postawę oraz rób regularne przerwy, aby chronić wzrok i układ mięśniowo-szkieletowy.

5. Postępowanie w Przypadku Problemów

ProLine S.A., ul. Brzozowa 5, 55-095 Mirków, NIP: 8951898022, KRS: 0000282071, Regon: 020482041, BDO: 000437899. Wpisana przez Sąd Rejonowy dla Wrocławia - Fabrycznej Wydział VI KRS pod nr: 0000282071. Kapitał zakładowy Spółki wynosi 500000 zł i został on opłacony w całości.

- **Podejrzenie Infekcji:** Jeśli podejrzewasz, że Twoje urządzenie lub pliki zostały zainfekowane złośliwym oprogramowaniem, natychmiast przeskanuj system programem antywirusowym i rozważ odłączenie urządzenia od sieci. Skontaktuj się z pomocą techniczną lub specjalistą ds. bezpieczeństwa.
- **Problemy Techniczne:** W przypadku problemów z działaniem oprogramowania, zapoznaj się z oficjalną dokumentacją, forum użytkowników lub skontaktuj się z pomocą techniczną producenta.

6. Zastrzeżenie

Producent ani dystrybutor oprogramowania nie ponoszą odpowiedzialności za szkody wynikające z nieprzestrzegania zasad bezpieczeństwa opisanych w niniejszej instrukcji, w tym za utratę danych, naruszenie bezpieczeństwa lub inne straty spowodowane niewłaściwym użytkowaniem, instalacją z nieautoryzowanych źródeł lub brakiem stosowania podstawowych środków ostrożności.

Pamiętaj: Bezpieczeństwo cyfrowe to proces ciągły. Bądź czujny i regularnie aktualizuj swoją wiedzę na temat zagrożeń oraz dobrych praktyk.