

7 PODSTAWOWYCH ZASAD PRACY ZDALNEJ



01. ZAPEWNIJ ODPOWIEDNIE WARUNKI

Stwórz takie warunki/stanowisko pracy, aby nikt nieupoważniony nie miał dostępu do komputera i danych (np. współlokatorzy, goście, ...). Nie korzystaj z komputera służbowego do celów prywatnych.

02. ZABEZPIECZ SWOJE DANE DOSTĘPOWE



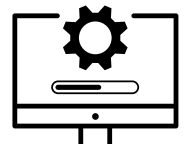
Pracuj na swoich danych dostępowych i stosuj silne hasła (zgodnie z procedurami obowiązującymi w Twojej organizacji). Nie zapisuj loginów i haseł w notesiku lub na kartkach samoprzylepnych, do których osoby nieupoważnione mogłyby mieć dostęp.



03. ZABLOKUJ DOSTĘP, GDY OPUSZCZASZ STANOWSIKO

Kończysz pracę, wyloguj się ze wszystkich usług/systemów/aplikacji i wyłącz komputer. Odchodzisz na chwilę od komputera, zawsze blokuj do niego dostęp.

04. AKTUALIZUJ SYSTEMY I PROGRAMY



Pamiętaj o aktualizacjach systemu operacyjnego i oprogramowania antywirusowego. Nie instaluj samodzielnie żadnych programów na służbowym laptopie.



05. KORZYSTAJ Z ZAUFANEJ SIECI WI-FI

Unikaj ogólnodostępnych sieci np.: w centrach handlowych, dworcach PKP i PKS, restauracjach, itp. Korzystając z sieci domowej, sprawdź czy Twoje hasło jest dość mocne. Nie stosuj łatwych do odgadnięcia wyrażań, np.: admin, 1234, 0000, imię, daty...

06. ZABEZPIECZ DOKUMENTACJĘ PAPIEROWĄ



Nie drukuj poza firmą dokumentacji służbowej, a jeśli już to zrobisz, zabezpiecz ją i zniszcz gdy przestanie być potrzebna. Nie zabieraj z firmy żadnej dokumentacji bez zgody przełożonego.

07. ZASADY E-MAIL



W komunikacji służbowej korzystaj tylko ze służbowych kont e-mail. Jeśli przesyłasz duże ilości danych osobowych i firmowych, zaszyfruj pliki (np. 7-Zip). Pamiętaj, aby hasło do plików przestać oddzielnie (np. SMS). Nie otwieraj podejrzanych e-maili, zwłaszcza tych zawierających dziwne linki i załączniki. Przed wysłaniem wiadomości sprawdź czy prawidłowo wpisałaś/eś adresatów wiadomości i nie zapomnij o opcji, która umożliwia ukrycie adresatów przed innymi odbiorcami wiadomości (UDW).



W razie wątpliwości i pytań skontaktuj się z osobami odpowiedzialnymi za bezpieczeństwo w Twojej firmie:

z Inspektorem Ochrony Danych

lub

w kwestiach technicznych z działem IT