**Niezbędne środki bezpieczeństwa danych osobowych przetwarzanych podczas wykonywania pracy w sposób zdalny.**

Administrator, mając na uwadze zapewnienie odpowiedniego poziomu bezpieczeństwa przetwarzania danych osobowych podczas pracy zdalnej, zobowiązuje pracownika do przestrzegania następujących zaleceń:

1. Zabezpieczenie komputera silnym hasłem (małe, duże litery, cyfry, znaki specjalne)
2. Regularne aktualizowanie systemu operacyjnego.
3. Zainstalowanie oprogramowania antywirusowego i aktualizowanie baz wirusów.
4. Ustawienie automatycznego blokowania komputera po 10 min nieaktywności.
5. Blokowanie komputera w przypadku każdego odejścia od stanowiska pracy.
6. Nieudostępnianie komputera osobom postronnym ( w przypadku korzystania ze sprzętu prywatnego do celów służbowych – założenie nowego konta użytkownika, zabezpieczonego hasłem, na którym będą przetwarzane dane osobowe).
7. Nie korzystanie z otwartych sieci Wi-Fi.
8. W przypadku korzystania z prywatnej (domowej) sieci Wi-Fi, odpowiednie zabezpieczenie sieci poprzez ustawienie silnego hasła dostępowego (małe, duże litery, cyfry, znaki specjalne).
9. Korzystanie tylko z poczty służbowej.
10. **Wysyłanie zaszyfrowanych załączników mailowych, zawierających dane osobowe**.

