ZAŁACZNIK NR 2

W celu podniesienia poziomu bezpieczeństwa informacji danych osobowych przetwarzanych podczas pracy zdalnej zaleca się:

1. Zabezpieczenie komputera silnym hasłem.
2. Korzystanie z managerów haseł.
3. Stosowanie szyfrowania dysku komputera.
4. Korzystanie z kont użytkowników bez możliwości instalacji oprogramowania.
5. Aktualizowanie systemu operacyjnego oraz oprogramowania użytkowego.
6. Stosowanie oprogramowania antywirusowego i aktualizowanie baz sygnatur wirusów.
7. Korzystanie z automatycznego blokowania komputera po krótkim okresie nieaktywności.
8. Blokowanie komputera w przypadku każdego odejścia od stanowiska pracy (możliwość szybkiej blokady w systemach Windows za pomocą skrótu klawiszowego WIN+L).
9. Stosowanie, o ile to możliwe, oprogramowania pozwalającego na podłączenie wirtualnej sieci prywatnej VPN (kwestia zapewnienia bezpieczeństwa transferowanych danych oraz możliwość dostępu do zasobów danych Pracodawcy).
10. Nieudostępnianie komputera innym osobom (nawet w przypadku korzystania ze sprzętu prywatnego do celów służbowych).
11. Niekorzystanie z otwartych sieci Wi-Fi.
12. W przypadku korzystania z prywatnej (domowej) sieci Wi-Fi, odpowiednie zabezpieczenie sieci poprzez ustawienie silnego hasła dostępowego oraz sprawdzenie oprogramowania routera Wi-Fi (w miarę możliwości aktualizacja jego oprogramowania).
13. Korzystanie tylko z poczty służbowej (odpowiednio zabezpieczonej poprzez szyfrowanie).
14. Unikanie mediów społecznościowych (np. Messenger Facebooka) jako środka komunikacji służbowej.
15. Niezapisywanie haseł dostępowych w przeglądarkach internetowych bez należytego szyfrowania.
16. Wykonywanie kopii zapasowych tylko na zabezpieczonych nośnikach (szyfrowany dysk lub pendrive).