Załącznik nr 2 do Zarządzenia Nr 2/2020 Kierownika MZBK w Sławkowie z dnia 7 kwietnia 2020 roku

**Zgoda na korzystanie z prywatnego sprzętu elektronicznego w celach służbowych w okresie wykonywania pracy zdalnej, o której mowa w ustawie z dnia 2 marca 2020 r. o szczególnych rozwiązaniach związanych z zapobieganiem, przeciwdziałaniem i zwalczaniem COVID-19, innych chorób zakaźnych oraz wywołanych nimi sytuacji kryzysowych**

Wyrażam zgodę na korzystanie z prywatnego sprzętu elektronicznego: model:……………………………..….. numer:……………………………………………….. w celu:………………………………………………………………………………………….. przez:……………………………………………………………………………………………

…………………………….

*Data i podpis pracodawcy*

**DOTYCZY: Wytyczne minimalnej, bezpiecznej konfiguracji sprzętu prywatnego użytkowanego do celów służbowych w ramach tzw. Telepracy lub pracy zdalnej.**

W celu bezpiecznego przetwarzania informacji, w tym danych osobowych na komputerach prywatnych w ramach tzw. pracy zdalnej zgodnie z ustawą z dnia 2 marca 2020 r. o szczególnych rozwiązaniach związanych z zapobieganiem, przeciwdziałaniem i zwalczaniem COVID-19, innych chorób zakaźnych oraz wywołanych nimi sytuacji kryzysowych wskazuje się następujące zasady postępowania:

1. Komputer prywatny musi posiadać aktualne oprogramowanie antywirusowe wraz z aktualną bazą wirusów.
2. System operacyjny Komputera musi być systemem posiadającym wsparcie producenta oraz posiadać zainstalowane wszystkie aktualizacje.
3. Komputer musi posiadać wydzielone konto użytkownika wraz z ustawionym hasłem (zgodnie z przyjętą polityką haseł), znanym tylko uprawnionemu do pracy zdalnej pracownikowi w celu odizolowania danych służbowych od danych prywatnych.
4. Konto to nie może być udostępniane członkom rodziny lub innym osobom nieupoważnionym.
5. Dane służbowe przechowywane będą w zaszyfrowanej części dysku na utworzonym koncie do pracy służbowej.
6. Dostęp zdalny do systemów wewnętrznych Pracodawcy musi być realizowany tylko podczas wykonywania służbowych czynności, po wykonaniu których Pracownik powinien zadbać o rozłączenie się z dostępu zdalnego.
7. Zestawiane połączenie zdalne będzie szyfrowanym kanałem VPN.
8. Przy przesyłaniu jakichkolwiek danych służbowych pocztą elektroniczną powinna być użytkowana służbowa skrzynka poczty elektronicznej dostępna przez Internet (stronę www).
9. Jeśli do przenoszenia danych elektronicznych użytkowane będą zewnętrzne nośniki danych (pendrive, dysk zewnętrzny itp.) nośnik musi być zabezpieczony programem kryptograficznym (np. Bitlocker lub VeraCrypt).
10. Urządzenie brzegowe (router operatora) wykorzystywane w domu do łączenia się z Internetem powinno zawierać Firewall.
11. Dopuszcza się podłączanie do służbowego komputera udostępnionego pracownikowi za pomocą pulpitu zdalnego.

Jeżeli zaistnieje taka niezbędna konieczność, dodatkowo wskazuje się na zasady dotyczące wynoszenia służbowej dokumentacji w formie tradycyjnej:

1. pracownik wynosząc dokumentacje musi sporządzić listę wynoszonych w danym dniu dokumentów odnosząc się do sygnatury sprawy lub innego numeru/opisu identyfikacyjnego dokumentacje,
2. dokumenty muszą być przenoszone w zamykanej torbie, w celu ich ochrony przed warunkami atmosferycznymi (np. zamoknięciem, rozwianiem itp.),
3. za bezpieczeństwo (poufność, integralność, dostępność) wyniesionej dokumentacji odpowiada Pracownik,
4. zabrania się wyciągania dokumentacji z torby w środkach komunikacji publicznej lub w samochodach,
5. korzystając z samochodu do przewożenia dokumentacji, torba z dokumentami powinna zostać schowana w bagażniku samochodu.

Pracownik, który zgodnie z poleceniem Pracodawcy zostanie skierowany do pracy zdalnej powinien złożyć oświadczenie stwierdzające znajomość powyższych zasad oraz spełnienie wymagań przez prywatny sprzęt.

Niniejszym oświadczam, że znane są mi zasady postępowania i bezpiecznego przetwarzania informacji, w tym danych osobowych ustalone przez Pracodawcę przy tzw. pracy zdalnej zgodnie z ustawą z dnia 2 marca 2020 r. o szczególnych rozwiązaniach związanych z zapobieganiem, przeciwdziałaniem i zwalczaniem COVID-19, innych chorób zakaźnych oraz wywołanych nimi sytuacji kryzysowych.

Oświadczam, że komputer, który będzie wykorzystywany do przetwarzania służbowych informacji spełnia stawiane wymagania w zakresie zabezpieczenia antywirusowego oraz konfiguracji osobnego konta chronionego hasłem.

…………………………………

*Data i podpis pracownika*