Załącznik nr 3
do Regulaminu pracy zdalnej wykonywanej
okazjonalnie przez pracowników
w Lubuskim Urzędzie Wojewódzkim

**Zasady ochrony informacji, w tym danych osobowych,
w pracy zdalnej**

I. OBOWIĄZKI DOTYCZĄCE UŻYTKOWANIA SPRZĘTU, NARZĘDZI PRACY, SIECI I SYSTEMÓW INFORMATYCZNYCH

1. Pracownik jest zobowiązany do:
   1) adekwatnego zabezpieczenia i ochrony przed uszkodzeniem, kradzieżą, zniszczeniem lub nieuprawnionym użyciem/dostępem powierzonego sprzętu i dokumentów;
   2) wykorzystywania powierzonego sprzętu, oprogramowania i środków łączności wyłącznie do celów służbowych;
   3) niekorzystania ze sprzętu służbowego w miejscach publicznych;
   4) stosowania regulacji wewnętrznych obowiązujących w Urzędzie, a w szczególności „Polityki Bezpieczeństwa Danych Osobowych" w tym m. in. „Instrukcji postępowania w sytuacji naruszenia ochrony danych osobowych" oraz „Instrukcji Zarządzania Systemami Informatycznymi";
   5) dbałości o bezpieczeństwo danych tj. zachowania ich poufności, integralności oraz dostępności;

2. Wykorzystanie sprzętu:
   1) do pracy możliwe jest wykorzystanie służbowego sprzętu komputerowego będącego własnością Urzędu lub prywatnego sprzętu komputerowego, który:
      a) został skonfigurowany przez informatyków Biura Obsługi Urzędu i Rozwoju Systemów Informatycznych do pracy zdalnej,
      b) posiada oprogramowanie do bezpiecznego połączenia z siecią Urzędu,
      c) posiada zainstalowany i aktualny program antywirusowy,
      d) posiada aktualny system operacyjny ze wsparciem producenta;
   2) komputerowy sprzęt służbowy należy transportować w sposób zapobiegający kradzieży, zagubieniu, zniszczeniu lub utracie;
   3) dostęp do komputera chroniony jest hasłem;
   4) nośniki pamięci (w tym dyski komputerów) używane do przetwarzania danych powinny być szyfrowane;
   5) instalowanie oprogramowania lub aplikacji na służbowym sprzęcie komputerowym lub telefonie jest możliwe tylko przez informatyków Biura Obsługi Urzędu i Rozwoju Systemów Informatycznych;
   6) pracownik nie może przetwarzać informacji służbowych na innych nośnikach niż udostępnione mu przez pracodawcę;

7) pracownik może używać narzędzi lub materiałów niezapewnionych przez pracodawcę pod warunkiem, że umożliwia to poszanowanie i ochronę informacji poufnych, innych tajemnic prawnie chronionych, danych osobowych oraz informacji, których ujawnienie mogłoby narazić pracodawcę na szkodę.
8) w przypadku wykrycia wirusa lub przestarzałego oprogramowania antywirusowego konieczne jest natychmiastowe skontaktowanie się z informatykami Biura Obsługi Urzędu i Rozwoju Systemów Informatycznych;
9) w przypadku awarii lub uszkodzenia powierzonego sprzętu, należy niezwłocznie przekazać go do Biura Obsługi Urzędu i Rozwoju Systemów Informatycznych.

3. Zasady bezpieczeństwa pracy w sieci Internet:
   1) zabronione jest łączenie się z Internetem za pośrednictwem darmowych, ogólnodostępnych hot spotów Wi-Fi;
   2) połączenie się z zasobami sieciowymi Urzędu możliwe jest wyłącznie za pomocą sieci VPN;
   3) po zakończeniu pracy należy wylogować się z systemów teleinformatycznych urzędu i rozłączyć połączenie VPN, a następnie zabezpieczyć sprzęt IT przed dostępem osób nieupoważnionych;
   4) pracownik jest zobowiązany do zapewnienia bezpiecznego połączenia z Internetem w przypadku, gdy nie wykorzystuje środków łączności dostarczonych przez Urząd.
4. Zasady bezpiecznego użytkowania poczty elektronicznej:
   1) hasła do poczty elektronicznej nie powinny być zapisywane przez przeglądarkę internetową;
   2) przy wysyłaniu wiadomości e-mail pracownik zobowiązany jest każdorazowo upewnić się co do poprawności wpisanych adresów;
   3) zabronione jest używanie prywatnych kont pocztowych do przetwarzania informacji.
5. Praca zdalna z dokumentami papierowymi odbywa się zgodnie z poniższymi zasadami:
   1) wypożyczanie dokumentacji przetwarzanej w formie papierowej z siedziby Urzędu, co do zasady, jest zabronione;
   2) w przypadku konieczności korzystania z dokumentacji przetwarzanej w formie papierowej, należy dokonać jej odwzorowania cyfrowego;
   3) pliki elektroniczne (skany, zdjęcia) będące cyfrową wersją dokumentacji papierowej można tworzyć i przechowywać wyłącznie na sprzęcie komputerowym oraz w systemach należących do pracodawcy.

II. ZABEZPIECZENIA ORGANIZACYJNE

1. Pracodawca przeprowadza, w miarę potrzeb, instruktaż i szkolenie w zakresie ochrony danych osobowych dla pracowników wykonujących pracę zdalną.

2. Do przetwarzania danych osobowych dopuszczeni mogą być jedynie pracownicy posiadający stosowane upoważnienie, którzy odbyli szkolenie z zasad przetwarzania i ochrony danych osobowych w warunkach pracy zdalnej oraz złożyli oświadczenie o zachowaniu w poufności danych osobowych oraz środków ich ochrony.
3. Pracownicy mogą przetwarzać dane osobowe tylko w celach związanych z wykonywaniem swoich obowiązków służbowych.
4. Praca zdalna odbywa się zgodnie z następującymi zasadami:
   1) wszelkie informacje, w szczególności dane osobowe i informacje prawnie chronione przetwarzane poza siedzibą Urzędu, powinny być zabezpieczone przed przypadkowym lub niezgodnym z prawem zniszczeniem, utraceniem, zmodyfikowaniem, nieuprawnionym ujawnieniem lub nieuprawnionym dostępem do nich;
   2) zabronione jest pozostawianie dokumentów oraz sprzętu służbowego bez nadzoru w miejscach publicznych, samochodach lub publicznych środkach transportu;
   3) miejsce pracy zdalnej, w którym pracownik przetwarza dane, jest obszarem chronionym i wymaga zastosowania odpowiednich zabezpieczeń.
5. Zabezpieczenia, o których mowa powyżej, mogą polegać w szczególności na:
   1) odseparowaniu miejsca pracy od dostępu osób nieupoważnionych;
   2) odseparowaniu miejsca przechowywania służbowego przenośnego sprzętu komputerowego oraz dokumentów służbowych od dostępu osób nieupoważnionych;
   3) uniemożliwieniu wglądu w dokumentację przez osoby nieupoważnione;
   4) prowadzeniu służbowych rozmów telefonicznych w sposób gwarantujący ich poufność.
6. Przy przetwarzaniu wszelkich informacji, a w szczególności danych osobowych należy kierować się następującymi zasadami dotyczącymi przetwarzania danych osobowych:
   1) zasada zgodności z prawem, rzetelności i przejrzystości;
   2) zasada ograniczenia celu;
   3) zasada minimalizacji danych;
   4) zasada prawidłowości;
   5) zasada ograniczenia przechowywania;
   6) zasada integralności i poufności;
   7) zasada rozliczalności.
7. Pracownik jest zobowiązany do natychmiastowego powiadomienia inspektora ochrony danych i bezpośredniego przełożonego o każdym incydencie naruszenia bezpieczeństwa danych.

III. WYMOGI W ZAKRESIE KOMUNIKACJI

1. Komunikacja odbywa się:
   1) telefonicznie, pracownik ma obowiązek przekierować połączenia przychodzące na numer telefonu użytkowany w miejscu świadczenia pracy zdalnej;

2) za pośrednictwem systemu pracy grupowej Zimbra (służbowej poczty elektronicznej, kalendarza);
3) zapewnionej przez pracodawcę platformy wideokonferencji Zoom;
4) dekretacji w systemie EZD PUW.