ZARZĄDZENIE NR 51 /2020
REKTORA
WARSZAWSKIEGO UNIWERSYTETU MEDYCZNEGO
z dnia 16 marca 2020 r.

w sprawie zasad bezpieczeństwa pracy zdalnej w związku z zapobieganiem rozprzestrzenianiu się wirusa SARS-CoV-2 wśród członków społeczności WUM

Na podstawie § 12 ust. 7 Statutu Warszawskiego Uniwersytetu Medycznego, w związku z ustawą z dnia 2 marca 2020 roku o szczególnych rozwiązaniach związanych z zapobieganiem, przeciwdziałaniem i zwalczaniem SARS-CoV-2, innych chorób zakaźnych oraz wywołanych nimi sytuacji kryzysowych (Dz.U. poz. 374 z 2020 r.) („Ustawa"), wprowadza się niżej wymienione zasady pracy zdalnej:

§ 1.

1. W związku ze stanem wyższej konieczności, pracownicy WUM w celu realizacji zadań służbowych, mogą wykorzystywać prywatny sprzęt komputerowy, smartfony, tablety, itp. - do pracy zdalnej, świadczonej poza miejscem jej stałego wykonywania.

2. Zdalny dostęp do komputera oraz systemów i zasobów informatycznych WUM może zostać udzielony pracownikowi w okresie czasowym do 29 marca 2020r., każdorazowo indywidualnie, na podstawie decyzji kierownika jednostki organizacyjnej.

3. Zdalny dostęp zapewnia Centrum Informatyki, po dokonaniu zgłoszenia na adres: IT@wum.edu.pl przez kierownika jednostki organizacyjnej.

§ 2.

1. Pracownik, wykorzystujący prywatny sprzęt, o którym mowa w § 1 ust. 1, zobowiązany jest do stosowania zasad bezpieczeństwa w obszarze przetwarzania danych osobowych oraz danych stanowiących tajemnicę przedsiębiorstwa, należących do Warszawskiego Uniwersytetu Medycznego, zgodnie z obowiązującą Polityką Bezpieczeństwa Informacji i z uwzględnieniem Zasad użytkowania sprzętu komputerowego, w tym przenośnych komputerów służbowych (laptopów), dysków (pamięci zewnętrznych, pendrive), pamięci w telefonach służbowych oraz tabletów służbowych WUM, stanowiącymi załącznik nr 2 do Zarządzenia Rektora nr 12/2020 z dnia 15 stycznia 2020 r.

2. Urządzenia i oprogramowanie wykorzystywane do realizacji zdalnego dostępu nie mogą zagrażać bezpieczeństwu udostępnionych przez WUM zasobów i muszą być chronione w sposób, który uniemożliwia bezpośrednie lub pośrednie pozyskanie przez osoby nieupoważnione dostępu do zasobów Uczelni.

3. Pracownik pracujący zdalnie zobowiązany jest do:

   1) zastosowania odpowiednich zabezpieczeń chroniących zasoby przed oprogramowaniem złośliwym (np. wirusami, robakami, backdoorami itd.), w szczególności:

      a) zainstalowania aktualizacji systemu oraz oprogramowania antywirusowego,

b) zastosowania silnego hasła (zalecane ponad 12 znaków z cyframi, małymi i dużymi literami oraz znakami specjalnymi),

c) wyeliminowania możliwości przejęcia kontroli nad urządzeniem lub jego wykorzystania w trakcie komunikacji z zasobami sieciowymi WUM,

2) niepodejmowania żadnych działań, które pośrednio lub bezpośrednio mogą prowadzić do naruszenia bezpieczeństwa udostępnionych zasobów Uczelni,

3) niewykorzystywania zasobów Uczelni ponad zakres niezbędny do wykonywania powierzonych obowiązków pracowniczych, wynikających z zakresu przyznanego dostępu.

4. Kanały komunikacyjne zestawiane na potrzeby dostępu do zasobów sieciowych Uczelni nie mogą być przez pracownika wykorzystywane w celu innym, niż wynikający z zakresu obowiązków, zarówno w zakresie czasowym, jak i w zakresie funkcjonalnym.

5. Pracownik korzystający ze zdalnego dostępu do systemów Uczelni ponosi pełną odpowiedzialność za swoje działania.

§ 3.

Zarządzenie wchodzi w życie z dniem podpisania.

Mirosław WIELGOŚ
REKTOR