

Zasady komunikacji wewnętrznej i bezpieczeństwa danych przetwarzanych w formie cyfrowej

§ 1.

1. W celu zapewnienia komunikacji wewnętrznej i załatwiania spraw, wprowadza się obowiązek przekazywania dokumentów w formie elektronicznej.
2. Zobowiązuje się wszystkich pracowników WUM do bieżącego, codziennego korzystania z poczty służbowej: imie.nazwisko@wum.edu.pl oraz zapoznawania się z przesyłaną za jej pośrednictwem korespondencją: sprawami, zarządzeniami, komunikatami, informacjami, czy dokumentami.
3. Kierownicy jednostek organizacyjnych są odpowiedzialni za nadzorowanie, aby każdy z pracowników jednostki, w tym osoby nowo zatrudniane, posiadał adres poczty służbowej i z niej regularnie korzystał.

§ 2.

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 do 30 września 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.
4. Kierownik jednostki organizacyjnej podejmuje decyzje w zakresie odebrania pracownikowi możliwości dostępu zdalnego do komputera oraz systemów i zasobów informatycznych WUM oraz składa w tej sprawie wnioski na adres: IT@wum.edu.pl

§ 3.

1. Ze względu na konieczność zapewnienia bezpieczeństwa przesyłanych danych, korzystanie z prywatnych adresów pocztowych w celach służbowych jest niedozwolone.
2. Wykonywanie pracy w formie zdalnej nie zwalnia pracowników z obowiązku stosowania i przestrzegania przepisów o ochronie danych osobowych.
3. Pracownik wykonujący pracę zdalną zobowiązany jest do niezwłocznego powiadomienia bezpośredniego przełożonego i IOD o wszelkich nieprawidłowościach w procesie przetwarzania danych osobowych.
4. Wnioski w sprawach pracowniczych wysyłane z prywatnych kont pocztowych, w tym o przyznanie pracownikowi świadczenia z ZFŚS, nie będą rozpatrywane.

§ 4.

1. W każdej jednostce organizacyjnej zlokalizowanej na terenie Kampusu Banacha należy zapewnić w godzinach pracy łączność telefoniczną, poprzez przekierowanie połączeń przychodzących na numery telefonów stacjonarnych w jednostce - na numery telefonów prywatnych odpowiednich pracowników wykonujących pracę zdalnie, z wyjątkiem jednostek .
2. Za organizację przekierowania połączeń odpowiadają kierownicy jednostek. Wsparcie w tym zakresie zapewnia Centrum Informatyki.
3. Zobowiązuje się Centrum Informatyki, we współpracy z Biurem Informacji i Promocji, do opracowania i udostępnienia na stronie internetowej:
 - 1) wykazu numerów telefonów kontaktowych do poszczególnych jednostek,
 - 2) wykazu adresów mailowych kontaktowych do najważniejszych jednostek administracji centralnej i wydziałowej, na które członkowie społeczności akademickiej mogą kierować sprawy do tych jednostek,
 - 3) zaleceń i rekomendacji dotyczących wyboru do stosowania optymalnych aplikacji ułatwiających pracę zdalną: dydaktyczną, naukową i administracyjną, typu: Teams, OneDrive, SharePoint, Zoom Video Communications,
 - 4) wytycznych dotyczących bezpieczeństwa informatycznego, w tym dotyczących pracy na sprzęcie prywatnym.

§ 5.

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.

§ 6.

1. W przypadku braku możliwości złożenia dokumentów w obowiązującej elektronicznej formie, dopuszcza się możliwość złożenia papierowej formy dokumentu w skrzynce podawczej.
2. Skrzynki podawcze są umieszczone na parterze holu głównego budynku Rektoratu przy ul. Żwirki i Wigury 61, przy stanowisku ochrony budynku.
3. W skrzynkach podawczych mogą być składane dokumenty zaadresowane do: kancelarii WUM, właściwego dziekanatu oraz do sekcji socjalnej – w przypadku braku możliwości przesłania dokumentu w formie elektronicznej.