

## Zasady komunikacji wewnętrznej i bezpieczeństwa danych przetwarzanych w formie cyfrowej

### § 1.

1. W celu zapewnienia komunikacji wewnętrznej i załatwiania spraw, przekazywanie dokumentów odbywa się wyłącznie w formie elektronicznej, z zastrzeżeniem ust. 5.
2. Zobowiązuje się wszystkich pracowników WUM do bieżącego, codziennego korzystania z poczty służbowej: [imie.nazwisko@wum.edu.pl](mailto:imie.nazwisko@wum.edu.pl) oraz zapoznawania się z przesyłaną za jej pośrednictwem korespondencją: sprawami, zarządzeniami, komunikatami, informacjami, czy dokumentami.
3. Pracownicy administracyjni zobowiązani są do stałego dostępu do poczty służbowej w godzinach pracy i bezzwłocznego reagowania na korespondencję.
4. 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.
5. W przypadku braku możliwości złożenia dokumentów w obowiązującej elektronicznej formie, dopuszcza się możliwość złożenia papierowej formy dokumentu we właściwej skrzynce podawczej.
6. Skrzynki podawcze są umieszczone na parterze holu głównego budynku Rektoratu przy ul. Żwirki i Wigury 61, przy stanowisku ochrony budynku.
7. W skrzynkach podawczych mogą być składane dokumenty zaadresowane do: kancelarii WUM, właściwego dziekanatu oraz do sekcji socjalnej.

### § 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, z zastrzeżeniem, że umożliwiała to poszanowanie i ochronę informacji poufnych i innych tajemnic prawnie chronionych, w tym tajemnicy przedsiębiorstwa lub danych osobowych, a także informacji, których ujawnienie mogłoby narazić pracodawcę na szkodę.
2. Zdalny dostęp do komputera oraz systemów i zasobów informatycznych WUM może zostać udzielony pracownikowi każdorazowo indywidualnie, na podstawie decyzji kierownika jednostki organizacyjnej.
3. Zdalny dostęp zapewnia Centrum Informatyki, po dokonaniu zgłoszenia na adres: [it@wum.edu.pl](mailto: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](mailto:it@wum.edu.pl)
5. Centrum Informatyki prowadzi na bieżąco rejestr przyznanych zdalnych dostępu.

### § 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 przypadku pracy zdalnej, należy zapewnić łączność telefoniczną, poprzez przekierowanie połączeń przychodzących na numery telefonów stacjonarnych w jednostce - na numery telefonów prywatnych odpowiednich pracowników wykonujących pracę zdalnie.
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 dostarczonego przez WUM, w sposób określony przez Centrum Informatyki,
    - 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. Kierownik jednostki organizacyjnej administracyjnej lub bibliotecznej, pracującej w systemie naprzemiennym obejmującym pracę zdalną, tworzy w programie Microsoft Teams zespół dedykowany do komunikacji wewnętrznej i pracy zdalnej dla tej jednostki.
2. Do zespołu należy dodać wszystkich pracowników jednostki organizacyjnej i przełożonych wyższego szczebla w stosunku do kierownika jednostki (np. dyrektor pionu, z-ca kanclerza, kanclerz).
3. Kierownik jednostki organizuje w aplikacji Microsoft Teams co najmniej raz w tygodniu spotkanie jednostki organizacyjnej, w którym uczestniczą wszyscy pracownicy, zarówno pracujący zdalnie, jak i stacjonarnie. W trakcie spotkania omawiane mogą być np. realizacja celów działu, realizacja zadań z danego tygodnia oraz plany na nadchodzący tydzień, status prac nad realizowanymi projektami, dokonywane są ustalenia dot. harmonogramu pracy zdalnej na najbliższy okres.
4. Kierownik jednostki umieszcza w plikach swojego zespołu Microsoft Teams harmonogram pracy zdalnej zespołu.