

Załącznik Nr 1
do Zarządzenia Nr 155/2026
z dnia 06.07.2026 r.
Rektora ŚUM

Regulamin korzystania z komputerów służbowych Śląskiego Uniwersytetu Medycznego w Katowicach

§ 1 Definicje

1. **Uniwersytet** – Śląski Uniwersytet Medyczny w Katowicach.
2. **Centrum Informatyki** – Centrum Informatyki i Informatyzacji SUM.
3. **Regulamin** – niniejszy Regulamin.
4. **Użytkownik** - osoba zatrudniona na podstawie umowy o pracę, na podstawie umowy cywilnoprawnej lub posiada status doktoranta Uczelni.
5. **Komputer służbowy** – stacjonarna stacja robocza, laptop lub inne urządzenie komputerowe (w tym urządzenie mobilne), przekazane Użytkownikowi do realizacji obowiązków służbowych.
6. **Konto Użytkownika** – konto w domenie/środowisku informatycznym Uczelni, wraz z przypisanymi uprawnieniami i zasobami.
7. **Dane służbowe** – wszelkie dane wytworzone, przetwarzane lub przechowywane w związku z wykonywaniem obowiązków służbowych, niezależnie od ich formy i nośnika.
8. **Nośnik zewnętrzny** – nośnik danych niebędący elementem Komputera służbowego (np. pendrive, dysk USB, karta pamięci).
9. **Incydent bezpieczeństwa** – zdarzenie skutkujące lub mogące skutkować naruszeniem poufności, integralności lub dostępności danych lub systemów (np. utrata/kradzież sprzętu, malware, phishing, nieuprawniony dostęp, podejrzenie wycieku).

§ 2 Postanowienia ogólne

1. Regulamin określa zasady korzystania z Komputerów służbowych oraz podstawowe obowiązki Użytkownika w zakresie bezpieczeństwa informacji i cyberbezpieczeństwa.
2. Regulamin stosuje się do wszystkich Użytkowników korzystających z Komputerów służbowych Uczelni.
3. Szczegółowe zasady ochrony informacji, w tym klasyfikacji danych, przechowywania i udostępniania, określają wewnętrzne polityki i procedury Uczelni. W przypadku sprzeczności stosuje się postanowienia zapewniające wyższy poziom bezpieczeństwa oraz zgodność z prawem.
4. Regulamin należy stosować łącznie z dokumentami obowiązującymi w Uczelni w obszarze SZBI/ochrony danych i bezpieczeństwa IT, w szczególności:
 - a) SZBI / System Zarządzania Bezpieczeństwem Informacji i ochrony danych osobowych,
 - b) Instrukcja klasyfikacji informacji,
 - c) Instrukcja Zarządzania Incydentami w Zakresie Bezpieczeństwa Informacji,
 - d) Regulamin sieci komputerowej SUMNET,
 - e) Regulamin użytkowania Elektronicznej Poczty Pracowniczej,
 - f) Instrukcja Bezpieczeństwa Pracy Zdalnej i Urządzeń Mobilnych oraz zasady i tryb wykonywania pracy zdalnej,
 - g) inne dokumenty powiązane opublikowane w rejestrze dokumentów Uczelni.
5. W przypadku rozbieżności pomiędzy dokumentami, pierwszeństwo mają postanowienia SZBI oraz instrukcji/procedur szczegółowych w zakresie bezpieczeństwa informacji i ochrony danych.
6. Użytkownik jest informowany o obowiązku stosowania Regulaminu przed rozpoczęciem korzystania z Komputera służbowego; informowanie może być realizowane m.in. poprzez komunikat systemowy przy logowaniu oraz przekazanie linku/lokalizacji dokumentu w procesie wydania sprzętu lub tworzenia konta.

§ 3 Zasady użytkowania

1. Powierzenie i przeznaczenie

1. Komputer może być powierzony Użytkownikowi do korzystania w miejscu pracy oraz – w uzasadnionych przypadkach – poza terenem Uczelni, zgodnie z zasadami obowiązującymi w Uczelni.
2. Komputer służbowy stanowi własność Uczelni i jest przeznaczony przede wszystkim do celów związanych z wykonywaniem zadań i obowiązków służbowych.
3. Osobą uprawnioną do korzystania z Komputera służbowego jest wyłącznie Użytkownik. W przypadku współdzielenia komputera przez więcej niż jednego Użytkownika, kierownik jednostki organizacyjnej wyznacza osobę odpowiedzialną za sprzęt.
4. Dopuszcza się incydentalne korzystanie z Komputera służbowego do celów prywatnych, o ile nie:
 - a) wpływa to na wykonywanie obowiązków służbowych,
 - b) narusza bezpieczeństwa informacji lub postanowień dokumentów wskazanych w §2 ust. 4,
 - c) powoduje instalowania nieautoryzowanego oprogramowania lub zmian konfiguracji,
 - d) generuje dodatkowych kosztów po stronie Uczelni,
 - e) wiąże się z przetwarzaniem lub przechowywaniem Danych służbowych w prywatnych usługach/nośnikach
5. Powierzenie Komputera służbowego do użytkowania poza lokalizacjami Uczelni następuje na podstawie wniosku realizowanego w systemie Elektronicznego Obiegu Dokumentów (EOD). Wniosek obejmuje opinię Centrum Informatyki, zgodę Zastępcy Kanclerza ds. Dydaktyczno-Informatycznych (lub osoby upoważnionej przez Rektora) oraz czynności ewidencyjne Działu Ewidencji Majątku.

2. Obowiązki Użytkownika – bezpieczeństwo i należyta staranność

1. Użytkownik jest zobowiązany właściwie eksploatować i dbać o powierzony mu Komputer służbowy oraz utrzymać go w stanie nie gorszym niż wynika to ze zwykłego zużycia eksploatacyjnego.
2. Użytkownik zobowiązany jest zabezpieczyć dostęp do komputera w sposób uniemożliwiający użycie przez osoby nieuprawnione, w szczególności poprzez:
 - korzystanie z indywidualnego konta i haseł zgodnych z wymaganiami Uczelni,
 - blokowanie ekranu przy każdorazowym odejściu od stanowiska,
 - ochronę informacji wyświetlanych na ekranie przed wglądem osób trzecich.
3. Użytkownik zobowiązany jest zabezpieczyć sprzęt przed utratą, kradzieżą, uszkodzeniem lub zniszczeniem (w tym niepozostawianie bez nadzoru w miejscach publicznych).
4. Zasady bezpiecznej pracy poza lokalizacjami Uczelni, w tym wymagania dotyczące połączeń sieciowych, urządzeń mobilnych i pracy zdalnej, określa Instrukcja Bezpieczeństwa Pracy Zdalnej i Urządzeń Mobilnych oraz zasady i tryb pracy zdalnej obowiązujące w Uczelni.

3. Dane służbowe i miejsce ich przechowywania

1. Wszystkie Dane służbowe wytworzone lub przechowywane na Komputerze służbowym w związku z wykonywaniem obowiązków są własnością Uczelni.
2. Użytkownik przechowuje Dane służbowe w rozwiązaniach wskazanych i udostępnionych przez Uczelnię (np. zasoby sieciowe, repozytoria, zatwierdzone usługi), zgodnie z Instrukcją klasyfikacji informacji oraz zasadami dotyczącymi danych badawczych, jeśli mają zastosowanie.

3. Zabrania się przechowywania lub przetwarzania Danych służbowych w prywatnych usługach chmurowych lub na prywatnych kontach, jeżeli Uczelnia zapewnia rozwiązania zatwierdzone, a także w sposób sprzeczny z dokumentami wskazanymi w §2 ust. 4.
4. Użytkownik przyjmuje do wiadomości, że dane przechowywane wyłącznie lokalnie na Komputerze służbowym mogą nie podlegać regularnemu tworzeniu kopii zapasowych. Użytkownik zobowiązany jest przechowywać Dane służbowe w lokalizacjach wskazanych i udostępnionych przez Uczelnię.

4. Oprogramowanie, konfiguracja, uprawnienia

1. Uczelnia udostępnia Użytkownikowi komputer z zainstalowanym systemem operacyjnym oraz oprogramowaniem. Konfiguracją komputerów, naprawą i wsparciem zajmuje się Sekcja Wsparcia Technicznego Centrum Informatyki.
2. Komputery mogą podlegać automatycznej ewidencji konfiguracji sprzętowej i zainstalowanego oprogramowania oraz kontroli stanu zabezpieczeń, zgodnie z SZBI i zasadami Uczelni.
3. Ze względów bezpieczeństwa Użytkownik co do zasady nie posiada uprawnień administracyjnych pozwalających na ingerencję w oprogramowanie i konfigurację systemu.
4. Użytkownikowi nie wolno samodzielnie zmieniać konfiguracji sprzętowej komputera, ustawień systemowych oraz instalować oprogramowania bez zgody Centrum Informatyki.
5. Użytkownik jest zobowiązany umożliwiać instalację aktualizacji systemowych i bezpieczeństwa oraz aktualizacji oprogramowania ochronnego, w tym wykonywać okresowe restarty Komputera służbowego, zgodnie z politykami Centrum Informatyki.
6. W przypadku oprogramowania instalowanego niestandardowo (za zgodą Centrum Informatyki) Użytkownik jest zobowiązany stosować się do zaleceń Centrum Informatyki w zakresie aktualizacji lub samodzielnie zapewniać aktualność tego oprogramowania, jeżeli Centrum Informatyki nie zapewnia jego automatycznej aktualizacji.
7. Użytkownik nie jest uprawniony do przenoszenia, udostępniania ani instalowania na innych urządzeniach oprogramowania lub licencji udostępnionych przez Uczelnię, chyba że warunki licencyjne oraz Centrum Informatyki wprost na to zezwalają.

5. Nośniki zewnętrzne i treści niedozwolone

1. W przypadku używania Nośników zewnętrznych Użytkownik zobowiązany jest wcześniej wykonać skanowanie programem ochronnym oraz stosować zasady obowiązujące w Uczelni (w tym dotyczące danych wrażliwych i szyfrowania, jeśli wymagane).
2. Użytkownik korzystający z komputera nie może przechowywać na nim danych oraz oprogramowania nielegalnego, jak również danych, informacji, materiałów mogących naruszać prawa osobiste lub majątkowe osób trzecich.
3. Centrum Informatyki może ograniczać dostęp do nieautoryzowanych Nośników zewnętrznych oraz stosować mechanizmy techniczne uniemożliwiające ich użycie na Komputerach służbowych.

6. Dostęp do zasobów służbowych, poczta i zasady kontroli

1. Uczelnia ma prawo wglądu do Danych służbowych oraz informacji zapisanych na Komputerze służbowym i w służbowych zasobach Użytkownika w zakresie niezbędnym do zapewnienia bezpieczeństwa, ciągłości działania, ochrony mienia i realizacji obowiązków Uczelni – zgodnie z SZBI i obowiązującymi przepisami.

2. Zasady korzystania ze służbowej poczty elektronicznej oraz zasady dostępu do służbowej skrzynki e-mail, w tym w okresie nieobecności Użytkownika, określa Regulamin użytkownika Elektronicznej Poczty Pracowniczej (w tym tryb wnioskowania i realizacji).
3. W przypadku zmiany jednostki organizacyjnej Użytkownik zobowiązany jest do przekazania spraw służbowych (w tym dokumentów i korespondencji) w sposób zapewniający ciągłość pracy, zgodnie z poleceniami przełożonego oraz obowiązującymi zasadami archiwizacji i obiegu dokumentów.

7. Zmiana miejsca użytkowania / przekazania majątku

W przypadku potrzeby zmiany miejsca użytkowania/jednostki organizacyjnej lub czasowego wypożyczenia Komputera służbowego należy postępować zgodnie z procedurami Działu Ewidencji Majątku (m.in. Procedura kontroli nr I/53 lub I/49 – zgodnie z aktualnym brzmieniem).

8. Incydenty bezpieczeństwa

Użytkownik ma obowiązek niezwłocznie zgłosić do Centrum Informatyki każdy Incydent bezpieczeństwa, w szczególności utratę/kradzież sprzętu, podejrzenie złośliwego oprogramowania, phishing, podejrzenie wycieku danych – zgodnie z Instrukcją Zarządzania Incydentami w Zakresie Bezpieczeństwa Informacji.

§ 4 Postanowienia końcowe

1. Użytkownik zobowiązany jest zwrócić Uczelni służbowy komputer w stanie nie pogorszonym poza zużycie wynikające z normalnej eksploatacji:
 - a. najpóźniej w dniu ustania stosunku pracy lub innego stosunku zobowiązaniowego łączącego go z Uczelnią,
 - b. na każde żądanie Uczelni.
2. W sytuacji opisanej w ustępie 1 lit. a. Użytkownik zobowiązany jest przekazać wszystkie dane zapisane na komputerze (dokumenty służbowe tworzone i przechowywane w pamięci komputera, pliki oraz inne posiadane informacje) związane z wykonywanymi zadaniami służbowymi przełożonemu lub do lokalizacji wskazanych przez Uczelnię.
3. Za nieprzestrzeganie postanowień Regulaminu wobec Użytkownika mogą zostać podjęte odpowiednie działania:
 - a. wobec pracowników - zgodnie z przepisami prawa pracy,
 - b. wobec osób na umowach cywilnoprawnych – zgodnie z postanowieniami umowy i przepisami prawa cywilnego,
 - c. wobec doktorantów - zgodnie z regulacjami wewnętrznymi Uczelni oraz przepisami powszechnymi.
4. W przypadku podejrzenia naruszenia prawa Uczelnia może dokonać zgłoszenia właściwym organom.
5. Użytkownik ponosi odpowiedzialność za powierzone mienie zgodnie z obowiązującymi przepisami prawa oraz regulacjami wewnętrznymi Uczelni, w zakresie szkód powstałych z winy umyślnej lub rażącego niedbalstwa, z uwzględnieniem zasad właściwych dla podstawy zatrudnienia.
6. Po zwrocie Komputera służbowego Centrum Informatyki może dokonać czynności serwisowych, w tym przywrócenia ustawień fabrycznych lub reinstalacji systemu, skutkujących trwałym usunięciem danych z nośników. Użytkownik jest zobowiązany przed zwrotem zapewnić

przekazanie Danych służbowych do lokalizacji wskazanych przez Uczelnię; Centrum Informatyki nie gwarantuje wykonania kopii zapasowej danych przechowywanych wyłącznie lokalnie.

7. Regulamin obowiązuje od dnia wejścia w życie Zarządzenia Rektora, do którego stanowi załącznik.

Rektor
Śląskiego Uniwersytetu Medycznego w Katowicach
prof. dr hab. n. med. Tomasz Szczepański