Załącznik do Zarządzenia Nr 4/2025
z dnia 13 stycznia 2025 r.

Spis paragrafów w regulaminie

1. *Postanowienia ogólne*
2. *Powierzenie komputera służbowego w użytkowanie*
3. *Autoryzacja użytkowników*
4. *Zasady korzystania z komputerów służbowych*
5. *Przechowywanie danych służbowych*
6. *Bezpieczeństwo dostępu do komputera i danych*
7. *Dostęp zdalny do zasobów i systemów*
8. *Konfiguracja komputerów*
9. *Wsparcie użytkowników*
10. *Wykorzystanie nośników pamięci zewnętrznej*
11. *Współdzielenie danych i praca grupowa On-Line*
12. *Zasady korzystania z udostępnionych usług IT*
13. *Zasady monitorowania pracy Pracowników przy wykorzystaniu komputerów służbowych*
14. *Postanowienia końcowe*

Regulamin korzystania z komputerów służbowych Pomorskiego Uniwersytetu Medycznego w Szczecinie

§ 1
Postanowienia ogólne

DZSI . . . . . Dział ds. Zintegrowanych Systemów Informatycznych PUM,
IOD . . . . . Inspektor Ochrony Danych PUM,
EZD . . . . . System Elektronicznego Zarządzania Dokumentacją w PUM,
VPN . . . . . Virtual Private Network (Wirtualna Sieć Prywatna) - bezpieczny tunel umożliwiający połączenie z dowolnego miejsca z infrastrukturą teleinformatyczną i zasobami PUM,
Użytkownik . Pracownik Uczelni posiadający komputer służbowy,
Domena . . . . Usługa katalogowa PUM, w ramach której Dział Informatyki zarządza uprawnieniami zasobów i użytkowników,

Niniejszy Regulamin określa zasady:

1. korzystania z komputerów służbowych włączonych do Domeny Pomorskiego Uniwersytetu Medycznego w Szczecinie (dalej : PUM, Uczelnia) lub infrastruktury teleinformatycznej Uczelni
2. korzystania z udostępnionych usług IT,
3. monitorowania pracy Użytkowników przy wykorzystaniu komputerów służbowych.

§ 2
Powierzenie komputera służbowego w użytkowanie

1. Komputer może być powierzony w użytkowanie osobie, która jest zatrudniona na podstawie umowy o pracę, na podstawie umowy cywilnoprawnej lub posiada status doktoranta Uczelni, zwanej w dalszej części Regulaminu Użytkownikiem.
2. Uczelnia powierza Użytkownikowi komputer stacjonarny do korzystania w miejscu pracy.
3. Uczelnia powierza Użytkownikowi komputer przenośny, który może być wykorzystywany poza miejscem pracy. W tym przypadku komputer powierzony jest na podstawie umowy powierzenia, której wzór stanowi załącznik nr 9 do Instrukcji gospodarowania mieniem oraz zasad odpowiedzialności za mienie Pomorskiego Uniwersytetu Medycznego w Szczecinie będącej załącznikiem do Zarządzenia Rektora Nr 73/2014.
4. Komputer przenośny może być wypożyczony pracownikowi czasowo na podstawie złożonego i zatwierdzonego wniosku, dla potrzeb realizacji zadań służbowych w trybie zdalnym.

5. Komputer powierzony Użytkownikowi stanowi własność Uczelni. Jako narzędzie pracy może być wykorzystywany wyłącznie do realizacji zadań służbowych i nie może być wykorzystywany do celów prywatnych.

§ 3
Autoryzacja użytkowników

1. Domena PUM (usługa katalogowa) to centralna baza danych kont użytkowników i komputerów, która jest zarządzana przez Dział Informatyki. Dzięki niej jest możliwość posługiwania się jednym kontem Użytkownika do logowania do wybranych systemów informatycznych (w tym do komputera służbowego).
2. Każdy Użytkownik pracujący w domenie PUM posiada indywidualne konto dostępowe, chronione silnym hasłem.
3. Określa się następujące reguły tworzenia hasła do konta Użytkownika w Domenie PUM:
    1) Minimalna liczba znaków w haśle: 12;
    2) Liczba zapamiętanych w systemie haseł: 2;
    3) Maksymalny okres ważności hasła: 180 dni;
    4) Maksymalna liczba nieudanych logowań: 10;
    5) Czas blokady konta po nieudanych próbach logowania: 30 minut;
    6) Hasło musi spełniać wymagania złożoności: małe znaki, cyfry, duże znaki lub znaki specjalne.
4. Logowanie do Domeny PUM odbywa się oparciu o ujednolicone nazwy Użytkowników tworzone wg przyjętej zasady: **imię.nazwisko@pum.edu.pl**.
5. Logowanie do komputera następuje po wprowadzeniu nazwy Użytkownika i hasła do domeny PUM. Nazwa Użytkownika i hasło przydzielane są w Dział Informatyki.

§ 4
Zasady korzystania z komputerów służbowych

1. Użytkownik korzystający z komputera nie może przechowywać na nim danych prywatnych, danych niezwiązanych z realizacją zdań służbowych, nielegalnego oprogramowania, jak również danych, informacji, materiałów mogących naruszać prawa osobiste lub majątkowe osób trzecich.
2. Na komputerach służbowych można używać wyłącznie oprogramowania znajdującego się na liście oprogramowania dopuszczonego do użycia w Uczelni. Lista takiego oprogramowania jest akceptowana przez władze Uczelni i dostępna w Intranecie PUM.
3. Osobą uprawnioną do korzystania z komputera jest wyłącznie Użytkownik.
4. Komputery służbowe ze względów bezpieczeństwa zabezpiecza się poprzez wprowadzenie ograniczeń uprawnień Użytkownika uniemożliwiających samodzielną instalację oprogramowania innego niż użytkowane na Uczelni lub zmiany konfiguracji komputera.
5. W szczególnych przypadkach Użytkownikowi mogą zostać nadane podwyższone uprawnienia do komputera służbowego. Uprawnienia takie nadawane są na podstawie wniosku, zaopiniowanego przez Dział Informatyki oraz Inspektora Ochrony Danych (IOD) i zaakceptowanego przez Rektora.
6. Dział Informatyki prowadzi ewidencję Użytkowników niebędących pracownikami Działu Informatyki/ZSI, którym nadano podwyższone uprawnienia do komputera służbowego.
7. Użytkownik posiadający podwyższone uprawnienia do komputera służbowego, odpowiada za właściwe użytkowanie tego komputera, stosowanie procedur z zakresu bezpieczeństwa teleinformatycznego oraz bezpieczeństwa informacji istniejących w Uczelni i ponosi konsekwencje ich niestosowania.
8. Użytkownikowi posiadającemu podwyższone uprawnienia do komputera służbowego nie wolno samodzielnie zmieniać konfiguracji sprzętowej komputera oraz ustawień w systemie operacyjnym, które mnogą naruszyć bezpieczeństwo teleinformatyczne danego komputera oraz infrastruktury teleinformatycznej Uczelni.

§ 5
Przechowywanie danych służbowych

1. Użytkownikowi pracującemu w Domenie PUM udostępnia się zasoby sieciowe indywidualne oraz współdzielone w postaci podłączonych dysków sieciowych:
   1) zasób indywidualny widoczny wyłącznie dla zalogowanego Użytkownika,
   2) zasób „razem" widoczny dla wszystkich pracowników danej komórki organizacyjnej,
   3) zasób „public" widoczny dla wszystkich Użytkowników w domenie PUM,

   na których powinny być przechowywane wszystkie dane służbowe.
2. Dla potrzeb obsługi zespołów lub grup roboczych mogą być utworzone dodatkowe zasoby sieciowe udostępniane dla Użytkowników będących członkami danych zespołów lub grup roboczych.
3. Dyski sieciowe mają ograniczenie maksymalnej pojemności, która domyślnie wynosi 10GB dla folderu wspólnego dla danej jednostki organizacyjnej oraz 1GB dla osobistego sieciowego folderu Użytkownika.
4. Dane na dyskach sieciowych są archiwizowane zgodnie z przyjętym planem kopii zapasowych i możliwe są do odzyskania w razie ich usunięcia.
5. Dodatkowo każdy pracownik PUM wraz z adresem służbowej poczty elektronicznej ma do dyspozycji dysk sieciowy w usłudze OneDrive systemu Microsoft 365 o pojemności 50GB na przechowywanie i współdzielenie danych umożliwiających pracę w trybie On-Line.
6. Przechowywanie ważnych danych służbowych tylko i wyłącznie na dysku lokalnym komputera jest niezalecane.
7. Dane i pliki służbowe przechowywane na dysku lokalnym komputera w razie awarii dysku lokalnego komputera będą niemożliwe do odzyskania.
8. W związku z powyższym Dział Informatyki rekomenduje przechowywanie danych służbowych na dyskach sieciowych.
9. Wszystkie dane zapisane na dysku komputera, na dyskach usług sieciowych lub na zewnętrznych nośnikach pamięci związane z wykonywanymi zadaniami służbowymi stanowią własność PUM.

§ 6
Bezpieczeństwo dostępu do komputera i danych

1. Użytkownik jest zobowiązany właściwie eksploatować i dbać o powierzony mu komputer oraz utrzymać go w stanie nie gorszym, niż wynika to ze zwykłego zużycia eksploatacyjnego.
2. Użytkownik zobowiązany jest do stosowania polityki czystego ekranu poprzez:
   1) Ustawienie monitorów stacji roboczych w taki sposób, żeby uniemożliwić osobom nieupoważnionym wgląd w zawartość ekranu;
   2) Niepozostawiania komputerów bez nadzoru lub w przypadku czasowego nieużywania, zablokowania komputera przed odejściem od stanowiska pracy.
3. Podczas tworzenia lub korzystania z haseł Użytkownik musi przestrzegać następujących zasad określonych w Polityce Ochrony Danych Osobowych PUM w szczególności:
   1) Hasła nie mogą być ujawniane innym osobom;
   2) Hasła mogą być zapisywane w sposób uniemożliwiający ich podejrzenie przez osoby nieupoważnione;
   3) Hasło musi zostać natychmiast zmienione, jeżeli istnieje podejrzenie, że hasło lub system informatyczny mógł zostać naruszony; Jeżeli Użytkownik nie może zmienić hasła musi niezwłocznie poinformować Dział Informatyki lub DZSI; Niezależnie od obowiązku zmiany hasła Użytkownik niezwłocznie informuje Dział Informatyki lub DZSI o podejrzeniu naruszenia hasła lub systemu informatycznego;
   4) Hasła muszą spełniać określone wymagania systemowe dotyczące używanych znaków;
   5) Hasło nie może być słowem słownikowym, pochodzącym z dialektu lub żargonu; w dowolnym języku, nie może być także słowem zapisanym wspak;
   6) Hasło nie może opierać się na informacjach osobistych takich jak data urodzin, imiona bliskich, numer telefonu;

7) Hasło nie może być zapamiętywane w aplikacjach lub przeglądarkach internetowych;
8) Hasła do urządzeń i systemów informatycznych muszą się różnić.

4. W celu zabezpieczenia danych znajdujących się na komputerze przenośnym (laptop) dyski komputerów szyfrowane są za pomocą funkcji typu “BitLocker”, a dostęp do nich zabezpieczony jest kodem PIN.

§ 7
Dostęp zdalny do zasobów i systemów

1. Dla potrzeb realizacji zadań służbowych w trybie zdalnym Użytkownik komputera może nawiązać połączenie z infrastrukturą teleinformatyczną PUM poprzez bezpieczne łącze VPN.
2. Przydzielenie uprawnień dostępowych poprzez VPN odbywa się zgodnie z procedurami określonymi w Zarządzeniu Rektora Nr 6/2025 z dnia 13 stycznia 2025 r. i odbywa się następująco:
   1) Dostęp do zasobów teleinformatycznych oraz wewnętrznych systemów informatycznych Uczelni dla pracowników Uczelni - na podstawie złożonego wniosku;
   2) Dostęp do zasobów bibliotecznych dla studentów i nauczycieli akademickich - na podstawie poświadczeń użytkownika z systemu Wirtualnego Dziekanatu;
   3) Dostęp do wyznaczonych zasobów teleinformatycznych Uczelni dla osób niebędących pracownikami Uczelni, firm/instytucji zewnętrznych w ramach zawartych umów na realizację konkretnych zadań lub świadczenie usług - na podstawie złożonego wniosku,
3. Wniosek podlega akceptacji Inspektora Ochrony Danych oraz Kanclerza .
4. Przydzielenie Użytkownikowi uprawnień dostępu zdalnego poprzez VPN realizuje Dział Informatyki.
5. Podczas połączenia zdalnego z infrastrukturą teleinformatyczną i zasobami PUM Użytkownik zobowiązany jest do zachowania należytego poziomu bezpieczeństwa w szczególności opisanego w § 6 ust. 2

§ 8
Konfiguracja komputerów

1. Pomorski Uniwersytet Medyczny w Szczecinie udostępnia Użytkownikowi komputer służbowy z zainstalowanym oprogramowaniem niezbędnym do realizacji zadań służbowych:
   1) Każdy nowy komputer dostarczany jest z pełnym pakietem biurowym składającym się między innymi z procesora tekstu, arkusza kalkulacyjnego, programu do prezentacji oraz klienta poczty elektronicznej;
   2) Każdy nowy komputer dostarczany jest z programem antywirusowym, który jest centralnie zarządzany przez Dział Informatyki i stanowi aktywną ochronę.
2. Każdy komputer służbowy konfigurowany jest do pracy w domenie PUM, przez co podlega grupowym zasadom i politykom bezpieczeństwa.
3. W szczególnych przypadkach za zgodą Rektora komputer służbowy może zostać odłączony od domeny PUM.
4. Odłączenie może nastąpić wyłącznie na podstawie wniosku, zaopiniowanego przez Dział Informatyki i zaakceptowanego przez Rektora.
5. Odłączony komputer traci dostęp do zasobów i systemów Uczelni wyszczególnionych w § 4 ust. 1-4.
6. Odłączenie komputera od domeny PUM skutkuje utratą jego nadzoru, stosowania reguł bezpieczeństwa i kontroli przez systemy nadzorowane przez Administratorów w Dziale Informatyki PUM.
7. Za bezpieczeństwo i eksploatację odłączonego od Domeny PUM komputera służbowego użytkujący go pracownik ponosi pełną odpowiedzialność.
8. Użytkownik komputera pracującego poza kontrolą Domeny PUM odpowiada za właściwe jego użytkowanie opisane w § 6, a także:
   1) Wykonanie cyklicznych aktualizacji oprogramowania antywirusowego;
   2) Wykonanie cyklicznych aktualizacji systemu operacyjnego.
9. Dział Informatyki prowadzi ewidencję zgłoszonych komputerów odłączonych od Domeny PUM i nie pracujących pod kontrolą Domeny PUM.

§ 9
Wsparcie użytkowników

1. Bieżące wsparcie Użytkowników komputerów służbowych świadczone jest przez pracowników Dział Informatyki oraz DZSI.
2. Wsparcie informatyczne może być świadczone w trybie zdalnym poprzez wykorzystanie narzędzi dostępu zdalnego do komputera w trybie nadzorowanym.
3. Dostęp zdalny do komputera Użytkownika realizowany jest za pomocą oprogramowania Team Viewer zarejestrowanego na PUM niewymagającego przekazywania przez Użytkowników danych i haseł dostępowych do komputera.
4. Dostęp zdalny do komputera odbywa się tylko i wyłącznie za zgodą Użytkownika zgłaszającego problem, który decyduje o udzieleniu dostępu.
5. W przypadku gdy bieżąca interwencja wymaga osobistego stawiennictwa pracownika na stanowisku pracy wsparcie takie może być realizowane przez:
    1) Informatyków z Działu Informatyki;
    2) Informatyków z DZSI;
    3) Informatyków z Działu Zaopatrzenia, którzy świadczą wsparcie dla użytkownika w lokalizacjach poza budynkiem Rektoratu PUM.
6. Dostęp do pomieszczeń Dział Informatyki i DZSI jest ograniczony kontrolą dostępu z uwagi na bezpieczeństwo systemów i przetwarzanych danych.
7. Problemy dotyczące komputerów i infrastruktury teleinformatycznej mogą być zgłaszane:
    1) Poprzez system ITRM;
    2) Telefonicznie - informatykom świadczącym wsparcie użytkowników (aktualne dane kontaktowe opublikowane są w serwisie Intranet PUM);
    3) Poprzez korespondencję e-mail na adres: informatyka@pum.edu.pl lub zsi@pum.edu.pl.
8. Usuwaniem usterek sprzętu komputerowego w Rektoracie PUM zajmuje się Dział Informatyki.
9. Usuwaniem usterek sprzętu komputerowego znajdującego się poza Rektoratem zajmują się informatycy z Działu Zaopatrzenia obsługujący jednostki zlokalizowane poza budynkiem Rektoratu.
10. W razie konieczności komputer z jednostki wydziałowej może zostać przekazany do Działu Informatyki w celu diagnostyki, naprawy lub poprawnej konfiguracji.

§ 10
Wykorzystanie nośników pamięci zewnętrznej

1. Ze względów bezpieczeństwa systemów informatycznych i infrastruktury teleinformatycznej Uczelni Zarządzeniem Rektora Nr 5/2025 z dnia 13 stycznia 2025 r. wprowadzone zostaje ograniczenie polegające na zablokowaniu dostępu do portów USB komputerów służbowych i obsługi zewnętrznych nośników pamięci (np. PenDrive, dyski zewnętrzne USB itp.) innych niż nośniki służbowe oraz zarejestrowane w centralnym systemie IT.
2. W związku ze specyfiką pracy niektórych jednostek organizacyjnych i specyfiką przetwarzanych przez nie danych - wyznaczone zostają stanowiska komputerowe objęte indywidualnym nadzorem, w ramach których możliwe jest podłączenie zewnętrznych nośników pamięci USB inne niż zarejestrowane.
3. Pracownicy tych jednostek pracujący na wyznaczonych komputerach odpowiadają za zachowanie szczególnych zasad bezpieczeństwa w związku z posiadanym uprawnieniem umożliwiającym wprowadzenie do infrastruktury teleinformatycznej PUM danych z nośników pamięci zewnętrznej w tym pochodzących spoza Uczelni.
4. Wymagane jest przeprowadzenie pełnego skanowania programem antywirusowym każdego podłączanego nośnika z danymi.
5. Wyjątkiem są wyznaczone komputery nieposiadające dostępu do wewnętrznych systemów teleinformatycznych PUM przeznaczone do prowadzenia prezentacji na Aulach i Salach konferencyjnych w wyznaczonych lokalizacjach.
6. W szczególnych i uzasadnionych przypadkach za zgodą Rektora na wskazanym komputerze służbowym może zostać wyłączone w/w ograniczenie obsługi nośników USB innych niż służbowe.

7. Wyłączenie ograniczenia na danym komputerze służbowym może nastąpić wyłącznie na podstawie wniosku, zaopiniowanego przez Dział Informatyki i zaakceptowanego przez Rektora.
8. Dział Informatyki prowadzi ewidencje wyznaczonych komputerów i użytkowników posiadających uprawnienia umożliwiające podłączanie zewnętrznych nośników pamięci USB innych niż nośniki służbowe.

§ 11
Współdzielenie danych i praca grupowa On-Line

1. Do wymiany korespondencji służbowej stosuje się Elektroniczny System Obiegu Dokumentów EZD (https://ezd.pum.edu.pl), który jest narzędziem wspomagającym dla tradycyjnego systemu kancelaryjnego na PUM.
2. System EZD dostępny jest w ramach wewnętrznej struktury teleinformatycznej PUM dla każdego pracownika Uczelni.
3. W przypadku konieczności uzyskania dostępu do systemu EZD z zewnątrz (spoza infrastruktury teleinformatycznej PUM) użytkownik łączy się przy wykorzystaniu połączenia VPN.
4. Fizyczny dostęp do plików i danych dla potrzeb realizacji zadań służbowych możliwy jest do uzyskania przy wykorzystaniu dostępnych na Uczelni narzędzi:
    1) Dostęp do dysków sieciowych za pomocą połączenia szyfrowanego VPN z komputerów służbowych z dowolnego miejsca z dostępem do Internetu;
    2) Dostęp do usługi OneDrive w systemie Microsoft365 umożliwiający pracę na dokumentach MS Office w trybie On-Line oraz współdzielenie tych zasobów pomiędzy pracownikami Uczelni.
5. Nadawanie użytkownikom uprawnień VPN odbywa się na podstawie wniosku podlegającego akceptacji IOD ora Kanclerza (szablon wniosku dostępny jest w Intranecie PUM oraz w systemie EZD),

§ 12
Zasady korzystania z udostępnionych usług IT

1. Usługi dedykowane dla Użytkowników pracujących w domenie PUM umożliwiają Użytkownikom korzystanie z zasobów informatycznych PUM.
2. Każdy Użytkownik pracujący w Domenie PUM posiada indywidualne konto dostępowe, chronione hasłem, którego udostępnianie osobom trzecim jest zabronione.
3. Za zarządzanie zasobami informatycznymi PUM (sprzętem, oprogramowaniem, danymi) i zapewnienie im bezpieczeństwa odpowiadają wyznaczeni pracownicy Dział Informatyki.
4. Za dodatkowe konfiguracje komputerów poza Rektoratem PUM odpowiadają informatycy w Dziale Zaopatrzenia obsługujący jednostki organizacyjne zlokalizowane poza budynkiem Rektoratu PUM.
5. Komputery nie będące własnością PUM wykorzystywane w celach naukowo-dydaktycznych przez osoby prowadzące zajęcia dydaktyczne mogą w ramach infrastruktury teleinformatycznej PUM uzyskać dostęp do Internetu.
6. Dostęp, o którym mowa w ust. 5 może zostać przydzielony na podstawie indywidualnego wniosku pracownika zawierającego dane komputera; w szczególności adres MAC karty sieciowej oraz dane Użytkownika komputera.
7. Dostęp, o którym mowa w ust. 5 nie obejmuje uprawnień dostępu do zasobów PUM, systemów informatycznych pracujących w Domenie PUM i przetwarzanych w nich danych.
8. Korzystanie z sieci komputerowej Uczelni podlega filtrowaniu ruchu sieciowego. Ruch związany z programami P2P oraz na portach uznanych za niebezpieczne jest blokowany.

§ 13
Zasady monitorowania pracy Pracowników przy wykorzystaniu komputerów służbowych

1. Uczelnia ma prawo wglądu do zapisanych na służbowym komputerze danych przy użyciu mechanizmów Domeny PUM.
2. W przypadku gdy Użytkownik zabezpieczył dane służbowe hasłem, na żądanie przełożonego zobowiązany jest je udostępnić.
3. Uczelnia zastrzega sobie prawo do instalacji na sprzęcie komputerowym oprogramowania do monitorowania legalności zainstalowanych programów.
4. Na żądanie Władz Uczelni – Administrator z Działu Informatyki może przekazać wskazanym osobom uprawnionym informacje dotyczące aktywności Użytkownika.

§ 14
Postanowienia końcowe

1. Użytkownik zobowiązany jest zwrócić Uczelni służbowy komputer w stanie niepogorszonym poza zużycie wynikające z normalnej eksploatacji:
    1) W przypadku komputera powierzonego pracownikowi w dniu ustania stosunku pracy lub innego stosunku łączącego go z PUM;
    2) Na każde żądanie Uczelni;
    3) W przypadku komputera wypożyczonego czasowo - na następny dzień roboczy po upływie okresu, na który komputer został wypożyczony.
2. W przypadku naruszenia postanowień regulaminu Użytkownik odpowiada odpowiednio przed Kanclerzem lub przed Rektorem.
3. W dniu ustania stosunku pracy lub innego stosunku łączącego pracownika z PUM, Użytkownik jest zobowiązany przekazać wszystkie dane zapisane w komputerze (dokumenty służbowe tworzone i przechowywane w pamięci komputera, pliki oraz inne posiadane informacje) związane z wykonywanymi zadaniami służbowymi przełożonemu.
4. Wyznaczenie przez kierownika danej jednostki organizacyjnej pracownicy, odpowiedzialni za realizacje zada, mogą uzyskać dostęp do danych przechowywanych przez pracownika w przypadku jego dłuższej nieobecności lub po rozwiązaniu stosunku pracy, na wniosek kierownika jednostki.
5. Pracownicy Działu Informatyki mogą dokonać kontroli przestrzegania postanowień niniejszego Regulaminu na polecenie Kierownika Dział Informatyki.
6. Każdorazowo z kontroli zostanie sporządzony protokół.
7. Korzystanie z sieci PUM podlega filtrowaniu ruchu sieciowego. Przy wejściu na potencjalnie niebezpieczną stronę Użytkownikowi wyświetlane jest ostrzeżenie.
8. Logi ruchu sieciowego zbierane są automatycznie przez logujące urządzenie zabezpieczające i przechowywane są przez okres 3 miesięcy zgodnie z Polityką Ochrony Danych Osobowych.
9. Zbiór informacji oraz dokumentów wraz z wytycznymi z zakresu bezpiecznej eksploatacji infrastruktury teleinformatycznej PUM dostępne są w Intranecie PUM (https://intranet.pum.edu.pl).

Załączniki:

- Załącznik 1: *Wniosek. Podłączenie komputera do Internetu*
  (dotyczy § 11, pkt 5)
- Załącznik 2: *Wniosek. Nadanie podwyższonych uprawnień do komputera służbowego*
  (dotyczy § 4, pkt 5)

prof. dr hab. Leszek Domański
Rektor PUM