załącznik nr 9 do Regulaminu studiów Uniwersytetu Medycznego
w Lublinie z dnia 22 kwietnia 2026 roku

Sporządził: Dział Ochrony Danych Centrum Informatyczne	**UNIWERSYTET MEDYCZNY W LUBLINIE**	**Zatwierdził:** Rektor Uniwersytetu Medycznego w Lublinie
Nazwa procedury: **PROCEDURA KORZYSTANIA Z SYSTEMU POCZTY ELEKTRONICZNEJ W UNIWERSYTECIE MEDYCZNYM W LUBLINIE – OSOBY STUDIUJĄCE**		**Wersja procedury:** **02**
Osoby realizujące: ADO, IOD, Kierownik CI, osoby studiujące		
Odniesienie do dokumentu bezpieczeństwa danych osobowych: Polityka Ochrony Danych UMLUB – Moduł III - Zarządzanie systemem informatycznym służącym do przetwarzania danych		

Definicje

UMLUB – Uniwersytet Medyczny w Lublinie.
Procedura – niniejsza procedura korzystania z systemu poczty elektronicznej Uniwersytetu Medycznego w Lublinie – osoby studiujące.
KP_S – konto pocztowe osoby studiującej.
SPU – system poczty elektronicznej Uniwersytetu Medycznego w Lublinie.
Użytkownik_S – użytkownik systemu poczty elektronicznej będący osobą studiującą Uniwersytetu Medycznego w Lublinie.
IOD – Inspektor Ochrony Danych Uniwersytetu Medycznego w Lublinie.
Kierownik CI – Kierownik Centrum Informatycznego **UMLUB.**
CI-UMLUB – Centrum Informatyczne Uniwersytetu Medycznego w Lublinie.
Konto specjalne – **KP_S** utworzone na potrzeby specjalnych wydarzeń np. konferencji. Dostęp do konta specjalnego posiada wyznaczona osoba i ona ponosi pełną odpowiedzialność za to konto.

załącznik nr 9 do Regulaminu studiów Uniwersytetu Medycznego w Lublinie z dnia 22 kwietnia 2026 roku

Postanowienia ogólne
1. Niniejsza Procedura określa zasady dostępu do **KP_S** w ramach **SPU** przez **Użytkownika_S**.
2. **SPU** dostępny jest dla wszystkich osób studiujących **UMLUB**, które zobowiązuje się do przestrzegania niniejszej procedury podczas korzystania ze **SPU**.
3. **CI-UMLUB** ma bezwzględny obowiązek niezwłocznego zamykania **KP_S Użytkowników_S**, którzy przestają być osobami studiującymi **UMLUB**, na podstawie powiadomienia o tym fakcie **Kierownika CI** przez właściwy Dziekanat **UMLUB**.
4. **KP_S** w domenie student.umlub.pl jest przeznaczone wyłącznie do celów, kontaktów oficjalnych do wykorzystania w sferze działalności edukacyjnej oraz wyłącznie na potrzeby **UMLUB**.
5. **Użytkownikowi KP_S** zabrania się: 1) wykorzystania **KP_S** do prywatnej działalności komercyjnej; 2) wysyłania treści niezgodnych z prawem; 3) zachowań niezgodnych z niniejszą Procedurą; 4) zachowań naruszających zasady współistnienia użytkowników sieci Internet.
6. **Użytkownik_S** ponosi pełną odpowiedzialność za: 1) wszelkie operacje wykonywane przy użyciu jego identyfikatora i hasła do **SPU**; 2) treści wysyłane przez siebie poprzez **SPU**; 3) skutki wejścia przez osoby trzecie w posiadanie hasła do **KP_S Użytkownika_S**, a zwłaszcza za ujawnienie hasła z winy **Użytkownika_S**.
7. **Użytkownik_S** zobowiązany jest do samodzielnego zabezpieczania poczty i danych przechowywanych na **KP_S**. **CI-UMLUB** nie odpowiada za utratę danych przez **Użytkownika_S** w **SPU**.

8. Korzystanie osoby studiującej ze **SPU** za pomocą **KP_S** oznacza, że jako osoba studiująca **UMLUB** posługująca się tym kontem zobowiązana jest do zachowania następujących zasad poufności informacji przesyłanych poprzez **SPU**:

1) zna i stosuje przepisy prawa regulujące zasady przetwarzania danych osobowych, w tym w szczególności Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 roku w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych), ustawy z dnia 10 maja 2018 roku o ochronie danych osobowych (Dz. U. z 2019 r.poz. 1781) oraz przepisy wszelkich aktów prawnych i procedur wewnętrznych **UMLUB**, jakie zostały jej przekazane do stosowania;

2) wie, że naruszenie integralności, dostępności, rozliczalności, niezaprzeczalności, a przede wszystkim poufności danych osobowych, w szczególności ujawnienie ich osobom nieuprawnionym, stanowi naruszenie ochrony tych danych i dołoży wszelkiej staranności by zapewnić ochronę danych osobowych przetwarzanych przez nią poprzez **SPU**;

3) wie, że pozyskiwanie przez nią danych osobowych bez upoważnienia osób, których dane dotyczą, nie wskazanie celu ich zbierania oraz wykorzystywanie tych danych do celów innych, niż do jakich zostały jej one przekazane, jest naruszeniem ochrony danych osobowych i zobowiązuje się do dołożenia szczególnej staranności przy dopełnianiu formalności podczas wnioskowania o dostęp do danych osobowych;

4) wie, że po przekazaniu jej przez **UMLUB** danych osobowych spoczywa na niej obowiązek ochrony tych danych, i wie, że jej obowiązek ochrony danych osobowych trwa również po ustaniu stosunku łączącego ją z **ULMLUB**;

5) wie, że naruszenie przez nią ochrony danych osobowych może stanowić podstawę odpowiedzialności karnej, cywilnej i dyscyplinarnej – w tym może stanowić podstawę do rozwiązania z nią stosunku łączącego ją z **UMLUB**.

9. Należy dołożyć szczególnej ostrożności przy korzystaniu z **KP_S**:

1) weryfikować adres nadawcy;
2) weryfikować odnośniki (linki) w treści wiadomości;
3) weryfikować załączone do wiadomości załączniki (program antywirusowy);
4) nie otwierać załączników mających podwójne rozszerzenie np. „wiadomość.pdf.zip”;
5) nie otwierać załączników pochodzących od nieznanego nadawcy, mających rozszerzenie: *.exe, *.scr, *.bat, *.com, *.pif (duże prawdopodobieństwo szkodliwego oprogramowania).

Polityka haseł

1. Dostęp do **KP_S** chroniony jest hasłem, które stanowi zabezpieczenie dostępu do **SPU** oraz treści i danych przechowywanych na **KP_S**. Hasło musi być bezwzględnie tajne tzn. znane jedynie **Użytkownikowi_S KP_S**. W przypadku podejrzenia odtajnienia hasła należy je niezwłocznie zmienić.

2. Hasło do **SPU** dla **Użytkowników_S** synchronizowane jest z hasłem domenowym. W przypadku kont specjalnych przechowywane jest w **SPU** i nie może być ono zbyt proste, łatwe do odgadnięcia przez osoby trzecie. Musi spełniać następujące warunki:

1) minimalna długość hasła - 12 znaków;

2) zawierać minimum 1 znak specjalny (tzn. !@#$%^&*()_+-={}[]”|’\<>?,./); 3) zawierać minimum 1 cyfrę; 4) zawierać minimum 1 wielką literę; 5) zawierać minimum 1 małą literę.
3. Zabronione jest stosowanie haseł: 1) będących nazwą użytkownika w jakiejkolwiek formie; 2) analogicznych jak identyfikator; 3) zawierających ogólnodostępne informacje takie jak imię, nazwisko, numer telefonu, imiona dzieci, numer rejestracyjny samochodu itp.; 4) będących słowami słownikowymi lub przewidywanymi sekwencjami znaków (np. 123456).
4. Zabronione jest łamanie haseł do **KP_S** innych **Użytkowników_S**.
5. Zabronione jest udostępnianie hasła do **KP_S** innym **Użytkownikom_S.**
6. Hasło musi być zmieniane nie rzadziej niż co 180 dni.
7. Hasło musi się różnić minimum 3 znakami od hasła poprzedniego.
8. Hasło nie może być hasłem, które Użytkownik stosował uprzednio – do 13 haseł wstecz.
Użytkowanie Konta Pocztowego
1. Użytkownicy **SPU** otrzymują adresy mailowe w domenie student.umlub.pl w postaci: nr_albumu@student.umlub.pl. W szczególnych przypadkach na wniosek opiekuna organizacji studenckiej możliwe jest utworzenie **Konta specjalnego**. Dostęp do tego konta przydzielony jest określonym osobom studiującym i oni ponoszą pełną odpowiedzialność za ich wykorzystanie.
2. Dostęp do **SPU** możliwy jest zarówno z poziomu przeglądarki pod adresem: https://poczta.student.umlub.pl/ lub za pomocą odpowiednio skonfigurowanego klienta pocztowego (np. Outlook, Thunderbird).

3. Korzystając z **KP_S Użytkownik_S** zobowiązuje się, że nie będzie działał w sposób naruszający prawa innych **Użytkowników_S** oraz nie będzie przenosił prawa do korzystania ze swojego **KP_S** na inne osoby.
4. Założenie **KP_S** następuje obligatoryjnie w momencie gdy **Użytkownik_S** staje się pełnoprawnym studentem.
5. Każdemu **Użytkownikowi_S** przyznane zostanie w **SPU** 130MB przestrzeni dyskowej na **KP_S**. W szczególnych przypadkach ta pojemność może zostać zmieniona.
Przesyłanie danych osobowych za pomocą KP_S
1. Przesyłanie danych osobowych za pomocą **KP_S** jest udostępnianiem, tj.: przetwarzaniem danych osobowych i odbywa się na zasadach określonych przepisami prawa, w szczególności Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 roku w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych), ustawy z dnia 10 maja 2018 roku o ochronie danych osobowych (Dz. U. z 2019 r. poz. 1781) oraz wewnętrznych aktów prawnych **UMLUB**.
2. Udostępnianie (przesyłanie) nie może naruszać praw i wolności osób, których dane dotyczą.
3. Dane osobowe mogą być udostępniane (przesyłane) wyłącznie odbiorcom uprawnionym do ich otrzymania: 1) na podstawie wniosku zawierającego m.in. podstawę udostępnienia oraz zakres udostępnionych danych.
4. **Użytkownik_S**, wnioskujący do nadawcy o udostępnienie mu (przesłanie) za pomocą **SPU** danych osobowych innych niż jego własne, w szczególności zgromadzonych w zbiorze lub zestawie danych, musi posiadać upoważnienia do ich pozyskania (przetwarzania) od wszystkich osób, których dane dotyczą.

W celu uprawdopodobnienia posiadania takiego upoważnienia zaleca się sporządzanie upoważnień pisemnych.
5. **Użytkownik_S** wnioskujący do nadawcy o udostępnienie (przesłanie) za pomocą **SPU** danych osobowych innych niż jego własne, w szczególności zgromadzonych w zbiorze lub zestawie danych, jest zobowiązany, na żądanie nadawcy do przedstawienia posiadanego przez siebie prawa do pozyskania (przetwarzania) tych danych.
6. Za weryfikację prawa **Użytkownika_S** do udostępnienia mu (przesłania) danych osobowych odpowiada nadawca, do którego **Użytkownik_S** wnioskował o udostępnienie (przesłanie) danych osobowych. Nadawca odmawia udostępnienia (przesłania) danych osobowych **Użytkownikowi_S**, jeżeli **Użytkownik_S** nie jest w stanie wykazać, że jest upoważniony do otrzymania danych osobowych, innych niż jego własne. Nadawca powiadamia o tym fakcie **IOD**, który po analizie okoliczności i potencjalnych skutków może podjąć decyzję o wszczęciu postępowania w sprawie naruszenia ochrony danych osobowych przez wnioskującego o udostępnienie danych osobowych.
7. Zabrania się wysyłania za pomocą **SPU** wiadomości zawierających w treści lub załącznikach dane osobowe przetwarzane w związku z tokiem studiów i działalnością edukacyjną, i w ramach struktury **UMLUB** na prywatne konta poczty elektronicznej.
8. Każdy **Użytkownik_S KP_S** – jako nadawca - zobowiązany jest do starannej weryfikacji odbiorcy wiadomości zawierającej dane osobowe.
9. Każdy **Użytkownik_S KP_S** – jako nadawca - zobowiązany jest do weryfikacji treści załączanych przez siebie do wiadomości plików, zawierających dane osobowe.
10. Każdy **Użytkownik_S KP_S** – jako odbiorca - zobowiązany jest do weryfikacji treści załączonych do otrzymanej wiadomości plików zawierających dane osobowe przed ich dalszym przetwarzaniem.

11. Każdy **Użytkownik_S KP_S**, który otrzymał wiadomość zawierającą dane osobowe, a która nie jest dla niego przeznaczona - zobowiązany jest niezwłocznie zawiadomić o pomyłce nadawcę tej wiadomości, zaś wiadomość odesłać do nadawcy a następnie ją usunąć.
12. Zabrania się wysyłania danych osobowych w treści wiadomości. W celu wysłania danych osobowych za pomocą **KP_S** należy utworzyć plik i załączyć go do wiadomości.
13. Zabrania się przesyłania za pomocą **KP_S** dokumentów zawierających dane osobowe, stanowiących załącznik do wiadomości bez zastosowania mechanizmów ochrony.
14. Przeznaczony do wysłania za pomocą **KP_S** dokument (dokumenty) zabezpiecza się hasłem. Odczytanie dokumentu jest możliwe po podaniu hasła. Hasła dostępowe ustala nadawca poczty zgodnie z Polityką haseł.
15. Hasło dostępowe wysyłane jest do adresata za pomocą: 1) SMS (zalecane); 2) przekazane ustnie przez telefon osobie upoważnionej do odbioru danych z zachowaniem ostrożności; 3) ustalone wcześniej, przed wysłaniem dokumentów; 4) ustalone w trakcie lub po wysłaniu dokumentów w sposób uniemożliwiający jego odgadnięcie osobom nieupoważnionym np. „hasło stanowią trzy pierwsze litery imienia i trzy pierwsze litery nazwiska oraz 4 ostatnie liczby numeru pesel osoby, której dane wysyłam” lub w sposób podobny; 5) w sytuacjach wyjątkowych uniemożliwiających zastosowanie żadnej z powyższych metod, w związku z koniecznością wysłania dokumentów – dopuszcza się wysłanie hasła na inny adres email wskazany przez odbiorcę bez informowania, że jest to hasło do dokumentu.
16. Udostępnianie (przesyłanie) danych osobowych niezgodnie z niniejszą Procedurą, skutkujące naruszeniem atrybutu poufności stanowi naruszenie

ochrony danych osobowych i podlega zgłoszeniu Prezesowi Urzędu Ochrony Danych.
Zasady odpowiedzialności – Użytkownik KP_S
1. Korzystając z konta pocztowego w domenie student.umlub.pl **Użytkownik_S** zgadza się na gromadzenie, przetwarzanie oraz wykorzystywanie podanych informacji o sobie przez **UMLUB** wyłącznie w celach technicznych, statystycznych.
2. **Użytkownik_S** ponosi pełną odpowiedzialność za treść i zawartość wiadomości przesyłanych za pomocą swojego **KP_S**.
3. **UMLUB** zobowiązuje się, że nie będzie udostępniał danych uzyskanych podczas korzystania z **KP_S** osobom trzecim. Wyjątkiem od tej zasady może być udostępnienie danych podmiotom uprawnionym do ich pozyskania na podstawie przepisów prawa.
4. **CI-UMLUB** zobowiązuje się dołożyć wszelkich starań w celu poprawnego działania **SPU** oraz zobowiązuje się do udzielenia wszelkiej pomocy **Użytkownikom_S** w problemach związanych z działaniem **SPU**.
5. **CI-UMLUB** zastrzega sobie prawo do: 1) awaryjnego wyłączenia systemu bez powiadomienia o tym fakcie **Użytkowników_S;** 2) zablokowania **KP_S** w przypadkach wykorzystania ich w sposób niezgodny z niniejszą Procedurą, a w szczególności za zmiany zasad działania **SPU** – zmiany takie zostaną ogłoszone wcześniej za pomocą **SPU** oraz na stronach **UMLUB**.
6. **CI-UMLUB** nie ponosi odpowiedzialności za: 1) utratę danych spowodowanych awarią sprzętu, systemu oraz innymi czynnikami niezależnymi od **CI-UMLUB**; 2) przerwy w działaniu **SPU** zaistniałej z przyczyn technicznych, konieczną konserwacją systemu oraz innych przyczyn niezależnych od **CI-UMLUB**. W przypadku konieczności wykonania prac konserwacyjnych w

SPU Użytkownicy zostaną o tym fakcie powiadomieni z odpowiednim wyprzedzeniem;

3) usunięcie przez Użytkownika **SPU** przetwarzanych przez siebie danych;
4) szkody wynikłe z niezgodnego z niniejszą Procedurą użytkowania **SPU**.