**Regulamin korzystania z systemu poczty elektronicznej**

**Uniwersytetu Medycznego im. Piastów Śląskich we Wrocław****iu**

**1. Przeznaczenie dokumentu**

Regulamin określa zasady użytkowania służbowej poczty elektronicznej (e-mail). Celem dokumentu jest ustanowienie obowiązujących wymagań w zakresie dozwolonego
i poprawnego korzystania z poczty e-mail, a także zminimalizowanie ryzyka dla ochrony danych przekazywanych drogą elektroniczną. Zasady określone w regulaminie obowiązują wszystkich użytkowników poczty służbowej.

**2. Zasady korzystania z poczty elektronicznej**

Główne zasady

2.1. Korzystanie ze służbowej poczty elektronicznej jest jednym ze sposobów realizowania obowiązków powierzonych użytkownikowi poczty i jest wykonywane wyłącznie w tych celach.

2.2. Korespondencja e-mail dot. spraw służbowych prowadzona jest wyłącznie przy pomocy adresu e-mail w domenie Uczelni „umw.edu.pl”. Zabronione jest korzystanie z innej, w tym prywatnej poczty e-mail w celach służbowych.

2.3. Wszystkie wiadomości e-mail wytworzone lub przysłane do użytkownika, związane
z wykonywaniem obowiązków służbowych, stanowią własność Uczelni i nie stanowią własności użytkownika.

2.4. Wykorzystywanie konta pocztowego zawierającego nazwę domeny Uczelni „umw.edu.pl” do celów korespondencji niezwiązanej z zatrudnieniem w Uczelni jest niedozwolone. Uczelnia nie wyraża zgody na wykorzystanie przez użytkowników służbowej elektronicznej skrzynki pocztowej w celach prywatnych lub związanych
z zatrudnieniem u innych pracodawców.

2.5. Użytkownicy poczty elektronicznej są odpowiedzialni za korzystanie z poczty w taki sposób, aby minimalizować ryzyko naruszenia bezpieczeństwa informacji.

2.6. W przypadku przesyłania informacji o szczególnym znaczeniu (np. poufnych, finansowych, danych badawczych, itd.) wewnątrz Uczelni bądź informacji wewnętrznych poza Uczelnię, należy w miarę możliwości wykorzystywać mechanizmy kryptograficzne (stosowanie haseł, szyfrowanie danych). Hasło umożliwiające odczytanie pliku, przesyła się za pomocą innego kanału komunikacji. Nie należy przekazywać w tej samej wiadomości e-mail jednocześnie zabezpieczonej informacji
i hasła.

2.7. Użytkownik jest uprawniony do korzystania tylko i wyłącznie z przydzielonego
lub przydzielonych mu adresów e-mail. Zakazane jest korzystanie z adresu e-mail innego użytkownika, a także logowanie się do skrzynki pocztowej innego użytkownika.

2.8. Wymagane jest okresowe porządkowanie skrzynki pocztowej poprzez usuwanie wiadomości zarchiwizowanych lub tych, które nie będą dłużej potrzebne,
w szczególności gdy w ich treści bądź załącznikach znajdują się dane osobowe.

2.9. Wszystkie nieprawidłowości w działaniu poczty elektronicznej, a także wątpliwości związane z korzystaniem z poczty elektronicznej, w tym związane z jej bezpieczeństwem, należy niezwłocznie konsultować z administratorem systemu pocztowego (CI).

2.10. Dane osobowe przesyłane drogą elektroniczną należy przekazywać w formie zaszyfrowanej lub w załączniku zabezpieczonym hasłem, zgodnie z opisaną
w regulaminie instrukcją.

Hasło do konta pocztowego

2.11. Użytkownik poczty elektronicznej nadaje hasło dostępu do konta.

2.12. Hasło nie powinny być powszechnie używanym słowem (słownikowe). Jako haseł nie należy wykorzystywać także: dat, imion, nazwisk, inicjałów, numerów rejestracyjnych samochodów, numerów telefonów.

2.13. Hasło składa się z co najmniej 8 znaków, zawiera małe i wielkie litery oraz cyfry
lub znaki specjalne.

2.14. Użytkownik konta zobowiązany jest zmienić swoje hasło nie rzadziej niż co 90 dni.

2.15. Hasła mają charakter poufny. Są znane tylko jego właścicielowi. Hasło nie może być ujawnione nawet po utracie przez nie ważności.

2.16. Zabronione jest zapisywanie haseł w sposób jawny oraz przekazywanie ich innym osobom.

Konfigurowanie wiadomości

2.17. W przypadku nieobecności należy ustawić "autoodpowiedź" zawierającą informację
o osobie, która zastępuje użytkownika w czasie nieobecności, do której nadawca może przesłać wiadomość.

2.18. Ustawienie automatycznego przekazywania wiadomości na adres innego pracownika jest niedozwolone (nie dotyczy adresów aliasowych).

2.19. Jeżeli kilku pracowników korzysta z ogólnego adresu e-mail, np. kontakt@, to każda wysyłana z takiego adresu wiadomość powinna zostać podpisana imieniem
i nazwiskiem osoby, która udziela odpowiedzi.

2.20. Jeżeli istotne jest potwierdzenie otrzymania przez adresata przesyłki, użytkownik powinien skorzystać z opcji systemu poczty elektronicznej informującej
o dostarczeniu i otwarciu wiadomości. Dodatkowo zaleca się, aby użytkownik zawarł w treści wiadomości prośbę o potwierdzenie otrzymania i zapoznania się
z informacją.

2.21. Użytkownicy nie powinni rozsyłać wiadomości zawierających załączniki o dużym rozmiarze do większej liczby adresatów. Określenie krytycznych rozmiarów przesyłek
i krytycznej liczby adresatów jest uzależnione od wydajności systemu poczty elektronicznej. W przypadku konieczności przesłania załącznika o dużym rozmiarze (np. filmu), w celu ustalenia sposobu dokonania przesyłki, należy korzystać z innych systemów uczelnianych lub skontaktować się z administratorem systemu pocztowego (CI).

Przesyłanie danych osobowych

2.22. W przypadku przesyłania plików zawierających dane osobowe do adresatów nieposiadających adresu e-mail w domenie Uczelni „umw.edu.pl”, dane osobowe należy przekazywać w zabezpieczonym hasłem załączniku do wiadomości. Użytkownik może zabezpieczyć załączane pliki poprzez ich kompresję i nadanie hasła archiwum wynikowemu.

2.23. Hasło służące do otworzenia i/lub modyfikacji pliku powinno zostać przekazane odbiorcy za pomocą innego kanału komunikacji, np. osobną wiadomością e-mail, wiadomością sms, drogą telefoniczną.

2.24. Hasło powinno być odpowiednio skomplikowane i niesłownikowe.

2.25. Dopuszczalne jest uzgodnienie stałego hasła w korespondencji z jednym odbiorcą.

2.26. Dopuszczalne jest zastosowanie jako hasła informacji, która jest znana tylko odbiorcy i której nie trzeba będzie przekazywać odrębną drogą komunikacji, np. znany odbiorcy numer ewidencyjny.

2.27. Przesyłając dane osobowe należy upewnić się, że:

a) dane nie są przesyłane w nadmiernym zakresie (często wystarczy imię i nazwisko
bez nr PESEL czy daty urodzenia),

b) prawidłowo określono adresatów,

c) temat wiadomości nie zawiera danych osobowych lub informacji poufnych.

Adresowanie wiadomości

2.28. Użytkownicy powinni zwrócić szczególną uwagę na poprawność adresu odbiorcy.
Za poprawność adresu odbiorcy odpowiedzialny jest nadawca wiadomości.

2.29. Przesyłanie informacji za pośrednictwem poczty elektronicznej powinno odbywać się zgodnie z uprawnieniami adresatów do korzystania z określonego typu informacji/danych. W przypadku wątpliwości nadawca powinien sprawdzić, czy dana osoba ma uprawnienia do korzystania z dokumentów danego typu lub o określonej klauzuli poufności poprzez skonsultowanie się z Działem Spraw Pracowniczych.

2.30. Przekazywanie wiadomości w sposób ujawniający dane adresatów (Do / Kopia) jest dozwolone tylko wówczas, gdy adresy e-mail odbiorców są adresami służbowymi lub są im wzajemnie znane i są zaangażowani w sprawę, której dotyczy wysyłana wiadomość.

2.31. W przypadku wysyłania wiadomości do kilku odbiorców, którzy nie znają wzajemnie swoich adresów e-mail i/lub korzystają z prywatnych adresów e-mail, należy te adresy wskazać w polu Ukrytej kopii. W takim wypadku wiadomość należy zaadresować
do siebie, wskazując swój adres e-mail w polu Do.

Działania zabronione

2.32. Zabrania się korzystania z poczty elektronicznej:

a) do wysyłania lub przechowywania wiadomości e-mail lub załączników, które mogą być uznane za nielegalne lub są powszechnie uznawane za obraźliwe
lub nieetyczne, w tym: obraźliwych komentarzy dotyczących rasy, płci, koloru skóry, niepełnosprawności, wieku, orientacji seksualnej, przekonań i praktyk religijnych, przekonań politycznych, narodowości,

b) do rozsyłania informacji niezwiązanych z wykonywanymi zadaniami, w tym zdjęć, filmików, żartów, "łańcuszków szczęścia", ostrzeżeń o wirusach, próśb o pomoc charytatywną, wirusów i innego złośliwego oprogramowania,

c) do oficjalnego reprezentowania pracodawcy bez odpowiedniego upoważnienia,

d) do wysyłania wiadomości e-mail z cudzego konta lub w cudzym imieniu,

e) do każdego innego niezgodnego z prawem, nieetycznego celu.

2.33. Zabronione jest uczestniczenie w przechwytywaniu, zapisywaniu, zmienianiu
lub ujawnianiu wiadomości e-mail należącej do innej osoby (nie dotyczy osób odpowiednio upoważnionych).

2.34. Zabronione jest przekierowywanie (forward i auto-forward) wiadomości e-mail
do innych systemów pocztowych.

**3. Zasady bezpieczeństwa**

3.1 Zabronione jest przesyłanie danych do logowania za pośrednictwem poczty elektronicznej. Centrum Informatyczne nie wysyła drogą mailową próśb o podanie danych do logowania.

3.2. Przed otwarciem wiadomości e-mail użytkownik powinien ustalić:

1. czy nadawca wiadomości jest mu znany i/lub czy otrzymywał wcześniej wiadomości od tego nadawcy,
2. czy spodziewał się otrzymać taką wiadomość,
3. czy tytuł, nazwa wiadomości i załącznika sugerują związek z wypełnianymi obowiązkami służbowymi.

Nie należy otwierać lub zwalniać z kwarantanny przesyłek budzących uzasadnione wątpliwości. W przypadku otrzymania takiej przesyłki, użytkownik powinien ją usunąć.

3.3. Należy pamiętać, że złośliwe oprogramowanie bywa przesyłane w postaci załączników lub pobierane jest po kliknięciu w zawarty w wiadomości link aktywujący. Dlatego, nie należy otwierać załączników (plików) lub linków nadesłanych przez nieznanego nadawcę, których odbiorca nie oczekiwał, nie mających związku z treścią wiadomości oraz wszystkich innych, które budzą uzasadnione wątpliwości. W celu weryfikacji prawidłowości korespondencji, użytkownik może skontaktować się
z nadawcą innym kanałem komunikacji (np. telefonicznie).

3.4. Zaleca się, w szczególności w przypadkach budzących wątpliwości użytkownika, weryfikację wiadomości za pomocą programu antywirusowego pod kątem obecności wirusów. Przed otwarciem należy zapisać plik na dysku, zweryfikować typ pliku
i sprawdzić programem antywirusowym. Nawet "bezpieczne" pliki (DOC, PDF) mogą zawierać wirusy.

3.5. Należy zwrócić szczególną uwagę na ataki phishingowe i fałszywe wiadomości e-mail.

*Phishing* to rodzaj oszustwa polegającego na wykorzystaniu naiwności osoby, z którą oszust się kontaktuje, w szczególności jej współczucia bądź chęci pomocy. Często przybiera formę podszywania się pod inną osobę lub instytucję w celu wyłudzenia informacji (np. danych dostępowych do systemów informatycznych, danych osobowych, informacji poufnych) czy zainfekowania urządzenia szkodliwym oprogramowaniem, a także skłonienia ofiary do pewnych działań, z reguły dla niej niekorzystnych. Dlatego bardzo uważnie należy czytać nadsyłane komunikaty
i analizować adresy e-mail, tj. czy są rzeczywiste, czy tylko łudząco podobne do adresów, z którymi zazwyczaj się kontaktujemy, jak np. adresów urzędów, banków, innych uczelni, itp.

3.6. Wiadomości SPAM, tj. niechciane lub niepotrzebne wiadomości powinny być przesyłane na adres e-mail: learn-is-spam@kwarantanna.umw.edu.pl i trwale usuwane.