**Procedury ochrony danych osobowych podczas wykonywania pracy zdalnej**

1. **Postanowienia ogólne**Niniejsze Procedury określają zasady przetwarzania danych osobowych, których administratorem jest Uniwersytet Medyczny im. Piastów Śląskich we Wrocławiu (dalej jako: „Pracodawca”), podczas wykonywania pracy zdalnej.

**II. Organizacja miejsca pracy**

1. Pracownik ma obowiązek organizacji miejsca wykonywania pracy zdalnej w sposób zapewniający ochronę danych osobowych.
2. W miarę możliwości pracę należy wykonywać w osobnym pokoju lub wyznaczonym do tego celu miejscu (np. przez faktyczne wydzielenie stanowiska pracy, osobne biurko, przeznaczone do przechowywania dokumentów lub innych nośników danych miejsce).
3. W przypadku chwilowego opuszczania pomieszczenia bądź stanowiska pracy, należy upewnić się, że do wykorzystywanych w trakcie pracy informacji nie będą miały dostępu osoby postronne, w tym domownicy. Należy zablokować dostęp do komputera i zabezpieczać dokumenty papierowe, np. poprzez umieszczenie ich w zamykanych szafkach.
4. Jeżeli pomieszczenie jest współdzielone z innymi domownikami, należy zapewnić, aby domownicy nie mieli wglądu w wykonywaną pracę, w szczególności poprzez właściwe ustawienie ekranu komputera, pracę z dokumentami w sposób uniemożliwiający wgląd.
5. Niedozwolone jest prowadzenie rozmów służbowych (telefonicznych, wideokonferencji) lub służbowej korespondencji w miejscach, które nie gwarantują zapewnienia poufności (np. winda, balkon, środki komunikacji publicznej czy inne miejsca dostępne publicznie).
6. Kończąc korzystanie ze służbowego telefonu należy upewnić się, że urządzenie zostało zablokowane.
7. Po zakończeniu pracy należy wyłączyć urządzenia elektroniczne i umieścić wszystkie elektroniczne i papierowe nośniki informacji (dokumenty) w szafkach, a jeśli to możliwe - zamykanych na klucz.
8. Niedozwolone jest podejmowanie pracy zdalnej w miejscach publicznych jak kawiarnie, restauracje, galerie handlowe, gdzie osoby postronne mogłyby usłyszeć fragmenty rozmów lub mieć wgląd w wykonywaną pracę.
	* 1. **Zasady pracy z dokumentacją w formie papierowej**
9. Pracownik ma obowiązek zapewnienia bezpieczeństwa dokumentacji przed wglądem osób nieupoważnionych (pozostawianie w sposób umożliwiający zapoznanie się z treścią) oraz przed zniszczeniem, uszkodzeniem, zabraniem przez osoby nieupoważnione. Dotyczy to także wszelkich kopii dokumentów.
10. Wszystkie wydruki, skanowane lub kopiowane dokumenty powinny być niezwłocznie usuwane z urządzeń, w celu uniemożliwienia zapoznania się z nimi osobom postronnym.
11. Po zakończonej pracy dokumenty należy przechowywać w bezpiecznym miejscu jak np. zamykane szafki, aktówki, teczki do przechowywania dokumentów, odkładane w miejsce poza zasięgiem domowników, w szczególności dzieci.
12. Obowiązuje ogólny zakaz wynoszenia dokumentów lub ich kopii poza teren zakładu pracy. Jeżeli do pracy zdalnej niezbędny jest dostęp do dokumentów, wyznaczony przez kierownika merytorycznej jednostki organizacyjnej pracownik wykonuje ich odwzorowanie cyfrowe.
13. W wyjątkowych przypadkach, gdy do pracy zdalnej niezbędny jest dostęp do dokumentów w formie papierowej, pracownik zgłasza do kierownika jednostki merytorycznej prośbę o możliwość ich skopiowania oraz wyniesienia poza teren zakładu pracy, na czas wykonywania pracy zdalnej. Po otrzymaniu zgody na piśmie (także w formie służbowej wiadomości e-mail), pracownik może sporządzić kopie niezbędnych dokumentów. Zabronione jest zabieranie poza teren zakładu pracy oryginałów dokumentów.
14. Po skopiowaniu dokumentów pracownik przygotowuje ich zestawienie, zawierające informacje jakie dokumenty, w jakiej liczbie zostały skopiowane. Informacja jest przekazywana kierownikowi merytorycznej jednostki organizacyjnej.
15. Podczas przewożenia dokumentów do miejsca wykonywania pracy zdalnej, należy zachować szczególną ostrożność i zabezpieczyć dokumenty przed ich zagubieniem, zniszczeniem, uszkodzeniem, zabraniem przez osoby nieupoważnione.
16. Niedozwolone jest wykonywanie pracy z dokumentami w miejscu publicznym (świetlica w szkole, kawiarnia, restauracja, galeria handlowa, itp.). Zabronione jest także korzystanie z ogólnodostępnych punktów ksero do powielania dokumentów zawierających dane służbowe, a w szczególności dane osobowe.
17. Po zakończeniu pracy, wykonane kopie dokumentów należy zwrócić kierownikowi merytorycznej jednostki organizacyjnej, który weryfikuje ich kompletność.
18. Zaleca się, aby praca zdalna była wykonywana wyłącznie w formie elektronicznej, tj. bez korzystania z wydruków roboczych dokumentów. W przypadku konieczności wykonania wydruku zawierającego dane osobowe, po zakończeniu pracy z dokumentem lub jego kopią, która nie jest dłużej potrzebna bądź nie wymaga archiwizowania, dokument należy niezwłocznie zniszczyć z wykorzystaniem niszczarki bądź przekazać do siedziby Pracodawcy celem zniszczenia w odpowiednich urządzaniach.

**IV. Bezpieczeństwo pracy zdalnej**

1. **Urządzenia stanowiące własność Pracodawcy (służbowe)**
2. Praca zdalna powinna być realizowana z wykorzystaniem urządzeń służbowych, tzn. otrzymanych od Pracodawcy: laptopa, komputera stacjonarnego, telefonu, tabletu, itp.
3. W przypadku narzędzi należących do Pracodawcy, do pracy zdalnej dopuszczone są wyłącznie komputery przygotowane przez Centrum Informatyczne.
4. Urządzenie służbowe jest udostępniane pracownikowi na potrzeby pracy zdalnej po spełnieniu warunków określonych w Instrukcji zarządzania siecią i systemami informatycznymi w UMW, stanowiącej załącznik nr 2 do zarządzenia nr 93/XV R/2018 Rektora Uniwersytetu Medycznego we Wrocławiu z dnia 1 sierpnia 2018 r.
5. Niedozwolone jest udostępnianie służbowych urządzeń wykorzystywanych do pracy zdalnej innym osobom, w tym domownikom.
6. Niedozwolone jest korzystanie z urządzeń służbowych do celów niezwiązanych z wykonywaniem obowiązków na danym stanowisku pracy.
7. Niedozwolone jest kopiowanie informacji służbowych na prywatne urządzenia.
8. Praca na komputerze wykonywana jest wyłącznie na koncie z ograniczonymi uprawnieniami, tj. koncie użytkownika.
9. Zalogowanie do systemu operacyjnego urządzenia wymaga uwierzytelnienia poprzez indywidualny login i hasło. Obowiązkiem pracownika jest zapewnienie poufności haseł dostępowych.
10. Poza przypadkami określonymi w regulacjach wewnętrznych Pracodawcy, niedozwolone jest korzystanie z jakiegokolwiek oprogramowania komputerowego innego niż oprogramowanie dostarczone przez CI, w szczególności dokonywanie instalacji takiego oprogramowania na urządzeniach.
11. Pracownik może korzystać z zewnętrznych nośników danych tylko po uprzednim sprawdzeniu zawartości nośnika oprogramowaniem antywirusowym.
12. Pracownik jest zobowiązany do zachowania szczególnej ostrożności podczas transportu urządzenia, w szczególności do zabezpieczenia go przed kradzieżą i dostępem osób nieuprawnionych.
13. **Urządzenia stanowiące własność pracownika (prywatne)**
14. Pracownik może wykonywać pracę zdalną za pomocą narzędzi pracy niezapewnionych przez Pracodawcę (urządzeń prywatnych) po podpisaniu i przekazaniu do Centrum Informatycznego oświadczenia stanowiącego załącznik nr 1 do niniejszego regulaminu.
15. W przypadku, gdy z urządzeń prywatnych wykorzystywanych do pracy zdalnej korzystają także inny domownicy, niezbędne jest wydzielenia osobnego konta użytkownika w systemie (pracownik wykonuje obowiązki służbowe wyłącznie w przeznaczonym do tego celu koncie użytkownika).
16. Zalogowanie do systemu operacyjnego lub konta użytkownika, o którym mowa powyżej wymaga uwierzytelnienia poprzez indywidualny login i hasło. Obowiązkiem pracownika jest zapewnienie poufności haseł dostępowych.
17. Pracownik może korzystać z zewnętrznych nośników danych tylko po uprzednim sprawdzeniu zawartości nośnika oprogramowaniem antywirusowym.
18. Pracownik wykonujący pracę zdalną za pomocą urządzeń prywatnych będzie miał dostęp wyłącznie do usług udostępnianych przez Pracodawcę w internecie.
19. **Minimalne wymagania w zakresie bezpieczeństwa:**
	1. urządzenie posiada legalne i aktualne oprogramowanie,
	2. urządzenie posiada włączone automatyczne aktualizacje oprogramowania,
	3. urządzenie posiada włączoną zaporę systemową,
	4. na urządzeniu został zainstalowany i działa w tle program antywirusowy,
	5. zalogowanie do systemu operacyjnego lub konta użytkownika wymaga uwierzytelnienia poprzez indywidualny login i hasło użytkownika,
	6. wyłączono autouzupełnianie i zapamiętywanie hasła w przeglądarce internetowej,
	7. został zainstalowany program umożliwiający zaszyfrowanie i odszyfrowanie danych (np. 7-zip),
	8. zostało zastosowane automatyczne blokowanie urządzenia po dłuższym braku aktywności.
20. **Opcjonalne wymagania w zakresie bezpieczeństwa:**

Pracodawca może dodatkowo wymagać, aby urządzenie wykorzystywane do pracy zdalnej zawierało inne zabezpieczenia, jak:

1. zaszyfrowany dysk,
2. wyłączone porty pamięci zewnętrznych,
3. oprogramowanie służące monitorowaniu wykonywania pracy przez pracownika, wykorzystywane zgodnie z wymaganiami przepisów prawa pracy.

**Internet**

1. W przypadku korzystania z domowej sieci WiFi, należy upewnić się, że została ona skonfigurowana w sposób minimalizujący ryzyko naruszenia poufności informacji, w szczególności:
	* + 1. korzystanie z internetu wymaga uwierzytelnienia poprzez hasło,
			2. hasło dostępowe składa się z co najmniej 8 znaków, w tym z dużych i małych liter oraz cyfr i znaków specjalnych,
			3. dostęp do panelu administracyjnego routera jest możliwy wyłącznie z urządzeń znajdujących się w sieci domowej,
			4. jeśli to możliwe, należy zmienić login do panelu administracyjnego routera na własny i zmienić domyślny adres routera na inny.

2. Niedozwolone jest korzystanie w trakcie wykonywanie pracy zdalnej z publicznych sieci WiFi o otwartym dostępie (np. w hotelach, restauracjach, komunikacji miejskiej, centrach handlowych, itp.).

**Zabezpieczanie informacji przesyłanych za pomocą poczty elektronicznej (e-mail)**

1. Wszelka korespondencja e-mail dot. spraw służbowych, prowadzona jest w trakcie wykonywania pracy zdalnej 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. Jeżeli informacje poufne, w szczególności dane osobowe, są przesyłane za pomocą poczty e-mail, powinny zostać udostępnione w załączniku zabezpieczonym hasłem. Hasło powinno być odpowiednio skomplikowane i niesłownikowe.
3. Rekomendowane metody zabezpieczania hasłem:
	* + - 1. nadanie hasła do pliku, w którym są dane osobowe,
				2. zabezpieczenie pliku lub plików poprzez kompresję z zabezpieczeniem archiwum wynikowego hasłem.
4. Zabezpieczeniu powinny podlegać wszelkiego rodzaju dane osobowe, niezależnie od ich charakteru, nawet jeżeli są to jedynie imiona, nazwiska, czy adresy e-mail.
5. Hasło do przesyłanego pliku zostaje przekazane odbiorcy inną drogą komunikacji.
6. Każda wiadomość powinna być wysyłana z należytą starannością, polegającą w szczególności na sprawdzeniu, czy jest kierowana do odpowiedniego odbiorcy. Za poprawność adresu odbiorcy odpowiedzialny jest nadawca wiadomości.
7. 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.
8. Szczegółowe zasady korzystania z systemu elektronicznej poczty pracowniczej (e-mail) określa odrębny Regulamin[[1]](#footnote-1).

**Zasady bezpiecznego prowadzenia wideokonferencji**

1. Do zainstalowania aplikacji na komputerze należy korzystać z oficjalnej strony aplikacji, a w przypadku urządzeń mobilnych z oficjalnego sklepu (Google Play lub App Store). W szczególności w przypadku przetwarzania danych osobowych, należy zwrócić uwagę czy rozmowy będą nagrywane i przechowywane, o jakie uprawnienia do danych użytkownik zostaje proszony (np. lista kontaktów, lokalizacja itp.) oraz czy aplikacja dysponuje niezbędnymi środkami bezpieczeństwa, takimi jak szyfrowanie.
2. Niedozwolone jest udostępnianie linków do wideo konferencji w mediach społecznościowych.
3. Jeśli to możliwe, należy włączyć domyślną ochronę spotkania on-line hasłem.
4. Należy upewnić się, że osoby postronne nie mają dostępu do ekranu.
5. Zaleca się korzystanie z opcji „poczekalnia” w celu uniknięcia dołączenia do wideokonferencji przypadkowych/niezaproszonych uczestników.
6. Przed udostępnieniem swojego ekranu podczas rozmowy należy zamknąć wszystkie okna, aby inni uczestnicy konferencji nie mieli do nich wglądu.
7. Niedopuszczalne jest udostępnianie dokumentów służbowych za pomocą czatu publicznego.
8. Logując się do telekonferencji, należy wyłączyć mikrofon i kamerę.
9. Po zakończeniu wideokonferencji należy:
10. wyłączyć mikrofon i kamerę,
11. upewnić się, że spotkanie zostało zakończone i zamknąć aplikację,
12. upewnić się, że program do telekonferencji nie działa w tle.

**V. Szczególne sytuacje**

* + 1. Problemy w działaniu urządzeń służbowych lub oprogramowania wykorzystywanych do wykonywania pracy zdalnej, należy niezwłocznie zgłaszać do CI.
		2. Pracownik zobowiązany jest do informowania bezpośredniego przełożonego o wszelkich problemach i utrudnieniach związanych z zapewnieniem właściwej ochrony danych osobowych.
		3. Jeżeli pracownik nie ma możliwości świadczenia pracy zdalnej z zapewnieniem właściwych zabezpieczeń, w szczególności ze względu na siłę wyższą, niezwłocznie zgłasza to bezpośredniemu przełożonemu i postępuje zgodnie z jego instrukcjami.
		4. W przypadku zgubienia lub kradzieży urządzeń, dokumentów lub innych nośników informacji, należy niezwłocznie, w dniu zdarzenia zgłosić je do:
1. Pracodawcy, e-mail: dg@umw.edu.pl
2. CI, e-mail: helpdesk@umw.edu.pl
3. inspektora ochrony danych, e-mail: iod@umw.edu.pl

5. Należy niezwłocznie zgłaszać bezpośredniemu przełożonemu i inspektorowi ochrony danych wszelkie podejrzenia naruszenia ochrony danych osobowych, jak np. utrata czy udostępnienie danych osobie nieuprawnionej, itd. Należy zgłaszać każdą sytuację, która w opinii pracownika odbiega od przyjętej normy i obowiązujących standardów bezpieczeństwa. Ocena ryzyka zdarzenia należy do Pracodawcy.

6. W przypadku wpłynięcia bezpośrednio do pracownika wykonującego pracę zdalną jakiegokolwiek żądania osoby, której dane dotyczą, pracownik przed podjęciem jakichkolwiek działań, konsultuje sposób postępowania, a w szczególności treść udzielanej odpowiedzi z inspektorem ochrony danych.

**VI. Szkolenie dot. Procedur ochrony danych osobowych podczas wykonywania pracy zdalnej**

1. Pracownik wykonujący pracę zdalnie, zobowiązany jest do odbycia szkolenia dot. Procedur ochrony danych osobowych podczas wykonywania pracy zdalnej, prowadzonego przez inspektora ochrony danych.
2. Dział Spraw Pracowniczych, przekazuje inspektorowi ochrony danych informację zawierającą wykaz osób zobowiązanych do odbycia szkolenia, o którym mowa powyżej, w terminie do 10 dnia miesiąca następującego po miesiącu, w którym pracownik rozpoczął wykonywanie pracy zdalnej.
3. Szkolenia odbywają się w formie e-learningu.
4. Pracownik zobowiązany do odbycia szkolenia, odbiera poprzez służbową elektroniczną skrzynkę pocztową, przekazany przez inspektora ochrony danych, dedykowany dla niego dostęp do materiału szkoleniowego.
5. Pracownik zobowiązany jest do odbycia szkolenia w terminie 7 dni od dnia otrzymania dostępu do materiału szkoleniowego.
6. Po ukończeniu szkolenia, pracownik w formie elektronicznej oświadcza zapoznanie się z zasadami ochrony danych osobowych zawartymi w materiale szkoleniowym i zobowiązuje się do ich przestrzegania.
7. Wygenerowane automatycznie przez elektroniczną aplikację szkoleniową oświadczenie, o którym mowa w pkt. 6 powyżej, udostępniane jest pracownikowi do wydruku. Drugi egzemplarz oświadczenia przechowywany jest w Dziale Spraw Pracowniczych.
1. Regulamin korzystania z systemu poczty elektronicznej Uniwersytetu Medycznego im. Piastów Śląskich we Wrocławiu, Załącznik nr 12 do Instrukcji zarządzania siecią i systemami informatycznymi UMW, Zarządzenie **nr 93/XV R/2018** **Rektora Uniwersytetu Medycznego we Wrocławiu** **z dnia 1 sierpnia 2018 r.**

 [↑](#footnote-ref-1)