Załącznik nr 3

do Regulaminu pracy zdalnej

w Uniwersytecie w Białymstoku

**Zasady ochrony danych osobowych na potrzeby pracy zdalnej**

1. **Procedury w zakresie bezpieczeństwa informacji i ochrony danych osobowych obowiązujące pracowników Uniwersytetu w Białymstoku (UwB) podczas wykonywania pracy zdalnej**

Procedura I – Ochrona informacji w miejscu wykonywania pracy zdalnej

1. Zasada bezpiecznej organizacji miejsca pracy:
2. przed rozpoczęciem pracy zdalnej należy wydzielić sobie odpowiednią przestrzeń, tak aby osoby postronne, nie miały dostępu do informacji
i dokumentów, nad którymi aktualnie pracujemy.
3. Zasada czystego biurka:
	1. dokumenty papierowe i nośniki komputerowe, kiedy nie są aktualnie używane, należy przechowywać w miejscach niedostępnych dla osób postronnych, w tym dla członków rodziny (np. przechowywanie
	w szafkach lub zamkniętych teczkach),
	2. należy ograniczyć do niezbędnego minimum ilość dokumentów zawierających dane osobowe, na których się pracuje,
	3. należy ograniczyć możliwość niekontrolowanego dostępu do przetwarzanych danych osobowych, w szczególności poprzez zamykanie teczek zawierających dane osobowe, odwrócenie tych dokumentów stroną zawierającą dane osobowe do dołu.
4. Zasada czystego ekranu:
	1. o ile to możliwe, monitor powinien być ustawiony w taki sposób, by osoby postronne nie miały możliwości wglądu do przetwarzanych aktualnie informacji,
	2. wygaszacze ekranu w stacjach roboczych powinny zostać aktywowane po okresie nieaktywności użytkownika trwającym maks. 15 minut,
	3. w przypadku opuszczenia stanowiska pracy należy zablokować stację roboczą, uniemożliwiając nieautoryzowany dostęp osób trzecich,
	4. z aplikacji zawierających dane osobowe i programów do obsługi poczty elektronicznej należy wylogować się bezpośrednio po zakończeniu
	w nich pracy.
5. Zasada poufności rozmów:
	1. w przypadku rozmów (również telefonicznych) dotyczących realizacji zadań prowadzonych poza obszarem uczelni należy zadbać, aby rozmowy nie były prowadzone w obecności osób nieupoważnionych do otrzymania tych informacji.
6. Zasada bezpiecznego korzystania z Internetu:
7. w przypadku korzystania z domowej sieci Wi-Fi lub Internetu w telefonie należy upewnić się, że zostały one skonfigurowane w sposób minimalizujący ryzyko uzyskania dostępu do sieci przez osoby nieuprawnione, w szczególności:
8. korzystanie z sieci powinno wymagać uwierzytelnienia poprzez hasło dostępu,
9. hasło dostępu powinno składać się z co najmniej ośmiu znaków, powinno zawierać duże i małe litery, cyfry oraz znaki specjalne,
10. domyślny adres routera powinien zostać zmieniony na inny,
11. niedopuszczalne jest łączenie się z niezabezpieczoną siecią publiczną,
12. przed rozpoczęciem korzystania z Internetu należy upewnić się, że system operacyjny jest zabezpieczony programem antywirusowym
i firewallem oraz że programy te są włączone,
13. wprowadza się całkowite ograniczenie w dostępie do treści uznanych za pornograficzne, rasistowskie, traktujące o przemocy, przestępstwach, jak również do protokołów umożliwiających wymianę plików w sieciach
z naruszeniem przepisów prawa.
14. jeżeli w realizowanej pracy niezbędne jest korzystanie z pamięci
w chmurze, dozwolone jest jedynie wykorzystywanie dysku Microsoft OneDrive na koncie UwB z zachowaniem wszelkich zasad i procedur dotyczących logowania i udostępniania danych (np. szyfrowanie danych osobowych przed umieszczeniem w chmurze).
15. Zasada bezpiecznego korzystania ze służbowej poczty elektronicznej:
16. korzystanie ze służbowej poczty elektronicznej dla celów prywatnych jest zabronione,
17. ponadto, zabronione jest:
18. odpowiadanie na wiadomości żądające podania danych niezbędnych do logowania się,
19. wysyłanie materiałów służbowych na konta prywatne w celu wykonywania pracy zdalnej,
20. wykorzystywanie systemu poczty elektronicznej do działań mogących zaszkodzić wizerunkowi UwB,
21. odbieranie przesyłek z nieznanych źródeł,
22. otwieranie załączników z plikami samorozpakowującymi się bądź wykonalnymi typu exe, com itp.,
23. przesyłanie pocztą elektroniczną plików wykonywalnych typu: bat, com, exe, plików multimedialnych oraz plików graficznych,
24. ukrywanie lub dokonywanie zmian tożsamości nadawcy,
25. odpowiadanie na niezamówione wiadomości reklamowe lub wysyłane łańcuszki oraz na inne formy wymiany danych określanych spamem, w przypadku otrzymania takiej wiadomości należy przesłać ją administratorowi systemu informatycznego,
26. posługiwanie się adresem służbowym e-mail w celu rejestrowania się na stronach handlowych, informacyjnych, chatach lub forach dyskusyjnych, które nie dotyczą zakresu wykonywanej pracy lub obowiązków umownych,
27. wykorzystywanie poczty elektronicznej do reklamy prywatnych towarów lub usług, działalności handlowo-usługowej innej niż wynikającej z potrzeb administratora danych lub do poszukiwania dodatkowego zatrudnienia,
28. informacje wrażliwe, a szczególnie dane osobowe, przed wysłaniem za pomocą wiadomości e-mail należy zaszyfrować,
29. załączniki do wiadomości e-mail należy przeskanować przed ich otwarciem,
30. kończąc pracę w programie pocztowym należy zawsze samodzielnie wylogować się z serwisu, klikając przycisk „wyloguj”,
31. należy zachować szczególną ostrożność w przypadku otrzymania wiadomości, gdy:
32. nie znamy nadawcy wiadomości,
33. tytuł wiadomości i nazwa załącznika budzą wątpliwości,
34. tytuł lub treść widomości napisana jest niepoprawnie pod względem gramatycznym lub stylistycznym.
35. Zasada bezpiecznego korzystania z dokumentacji służbowej:
	1. jeżeli do pracy zdalnej niezbędny jest dostęp do dokumentów zawierających dane osobowe w formie papierowej, pracownik zgłasza do pracodawcy prośbę o możliwość ich skopiowania oraz zabrania na czas wykonywania pracy zdalnej,
	2. po otrzymaniu zgody na piśmie lub w formie służbowej wiadomości e-mail, pracownik może sporządzić kopie niezbędnych dokumentów,
	3. zabronione jest zabieranie poza siedzibę pracodawcy oryginałów dokumentów,
	4. po skopiowaniu niezbędnych dokumentów, pracownik przygotowuje ich zestawienie, zawierające informacje jakie dokumenty oraz w jakiej liczbie zostały skopiowane i przekazuje je przełożonemu,
	5. podczas przewożenia dokumentów do miejsca realizowania pracy zdalnej należy zachować szczególną ostrożność, aby zapewnić ich poufność oraz bezpieczeństwo, w szczególności dokumenty powinny być przewożone w zamykanych teczkach lub kopertach w taki sposób, aby zapobiec ich zgubieniu, kradzieży oraz dostępowi przez osoby postronne,
	6. po zakończeniu pracy na dokumentach zawierających dane osobowe należy je zwrócić pracodawcy poprzez przekazanie ich przełożonemu lub po uzyskaniu zgody, zniszczyć w niszczarce do papieru w siedzibie pracodawcy.

Procedura II – Korzystanie ze sprzętu służbowego podczas wykonywania pracy zdalnej

1. Zasada bezpieczeństwa sprzętu służbowego użytkowanego poza siedzibą UwB:
	1. korzystanie ze środków przetwarzania informacji poza siedzibą UwB jest autoryzowane przez przełożonego,
	2. w odniesieniu do ochrony sprzętu znajdującego się poza siedzibą UwB, wprowadza się następujące wytyczne:
		1. nie należy pozostawiać bez nadzoru urządzeń lub nośników wynoszonych poza siedzibę UwB w celu ich ochrony przed dostępem osób nieuprawnionych,
		2. należy przestrzegać instrukcji producenta dotyczących ochrony sprzętu, np. ochrony przed wystawieniem na silne pola elektromagnetyczne,
		3. należy stosować odpowiednie zabezpieczenia określone
		w procesie szacowania ryzyka, niezbędne podczas pracy w domu,
		np. zamykane szafki, polityka czystego biurka, zabezpieczenie dostępu do komputerów oraz bezpieczne połączenie z UwB,
		4. nie należy instalować aplikacji pochodzących z nieznanych źródeł,
	3. zaleca się, aby przy wyborze właściwych zabezpieczeń uwzględnić fakt, że ryzyko, np. uszkodzenia, kradzieży lub podsłuchu, może znacząco różnić się w zależności od miejsca użytkowania sprzętu,
	4. należy pamiętać, że urządzenia i oprogramowanie przekazane przez pracodawcę do pracy zdalnej służą do wykonywania obowiązków służbowych. Obowiązuje więc zakaz wykorzystywania ich w celach prywatnych bądź przez osoby trzecie, w tym także przez członków rodziny.
2. Sprzęt komputerowy, urządzenia mobilne i dyski zewnętrzne powinny być zabezpieczone hasłem oraz posiadać szyfrowaną partycję służącą do przechowywania danych. Dane te powinny być zaszyfrowane w sposób uniemożliwiający ich bezpośrednie odczytanie przez osoby trzecie w przypadku utraty urządzenia.
3. Należy podjąć szczególne środki, aby urządzenia wykorzystywane podczas pracy zdalnej, szczególnie te wykorzystywane do przenoszenia danych, jak dyski zewnętrzne, nie zostały zgubione czy też skradzione.
4. W przypadku zgubienia lub kradzieży sprzętu komputerowego, urządzenia mobilnego bądź dysku zewnętrznego pracownik zobowiązany jest do natychmiastowego zgłoszenia incydentu naruszenia bezpieczeństwa zgodnie
z procedurą opisaną w § 12 Załącznika nr 1 do [Zarządzenia nr 11 Rektora Uniwersytetu w Białymstoku z dnia 16 kwietnia 2019 r. w sprawie wprowadzenia Polityki bezpieczeństwa danych osobowych oraz Instrukcji zarządzania Systemem informatycznym w Uniwersytecie w Białymstoku.](https://uwb.edu.pl/fcp/kFBsTMCQZEyUgCg4WSHd4ak1VYTZUNlAGDzRMdEFdZGhWG09gJxIYIXZvRQIGbyc/_global/public/main/pliki/zarzadzenie_nr_11.pdf)
5. Naruszenie regulacji w zakresie bezpieczeństwa sprzętu mobilnego jest traktowane jako naruszenie obowiązków służbowych i może skutkować odpowiedzialnością dyscyplinarną.

Procedura III – Korzystanie ze sprzętu prywatnego podczas wykonywania pracy zdalnej

1. W przypadku konieczności pracy zdalnej z wykorzystaniem komputera prywatnego wprowadza się zakaz zapisywania na nim bądź na prywatnych nośnikach informacji jakichkolwiek plików z danymi wrażliwymi (dane osobowe, informacje niejawne lub inne dane istotne z punktu Uczelni).
2. Cała praca może być zapisana wyłącznie na udostępnionych zdalnie pulpitach komputerów znajdujących się w zasobach zarządzanych przez UwB lub na zarejestrowanych zgodnie z procedurą nośnikach danych.
3. W celu wykonywania pracy zdalnej przy wykorzystaniu sprzętu prywatnego należy ustanowić na sprzęcie prywatnym odrębny profil pracowniczy.
4. Podobnie jak w przypadku komputerów służbowych należy zweryfikować, czy komputer prywatny jest zabezpieczony poprzez używanie silnych haseł, co pozwoli na ograniczenie dostępu do urządzenia, a jednocześnie na ograniczenie ryzyka utraty danych w przypadku kradzieży lub zgubienia urządzenia. Hasło powinno składać się z co najmniej ośmiu znaków i powinno zawierać duże i małe litery, cyfry oraz znaki specjalne.
5. Przed rozpoczęciem korzystania z komputera prywatnego w celach służbowych należy upewnić się że system operacyjny jest zabezpieczony programem antywirusowym i firewallem oraz że programy te są włączone. Muszą one być włączone przez cały czas korzystania z komputera prywatnego w celach służbowych.
6. Realizacja pracy zdalnej z prywatnego komputera poprzez dostęp do krytycznych systemów informatycznych jest dozwolona tylko w szczególnych przypadkach, po spełnieniu poniższych wymagań i tylko według opisanego poniżej schematu:
	1. przekazanie przez przełożonego w formie pisemnej listy osób oddelegowanych do pracy zdalnej w systemie administratorowi tego systemu,
	2. przedstawienie przez pracownika administratorowi systemu stałego adresu IP przydzielonego przez dostawcę Internetu, z którym pracownik ma zawartą umowę i z którego pracownik będzie nawiązywał połączenie do UwB,
	3. wystawienie przez UwB certyfikatu OpenVPN umożliwiającego podłączenie do sieci wewnętrznej UwB; ważność certyfikatu nie powinna być dłuższa niż rok, z możliwością przedłużenia na kolejny rok,
	4. zainstalowanie i skonfigurowanie na komputerze prywatnym pracownika aplikacji klienckiej OpenVPN, do połączenia z siecią wewnętrzną UwB,
	5. po uzyskaniu połączenia OpenVPN z komputera prywatnego, inicjowanie połączenia przy użyciu zdalnego pulpitu na komputer znajdujący się w zasobach UwB,
	6. w celu minimalizacji ryzyka wycieku danych osobowych, dostęp do systemów UwB może być realizowany wyłącznie za pomocą zdalnego pulpitu dostępnego poprzez połączenie OpenVPN,
	7. cała praca może być wykonana i zapisana wyłącznie na udostępnionych zdalnie pulpitach komputerów znajdujących się w zasobach zarządzanych przez UwB,
	8. po zakończonej pracy należy wylogować się z systemów dziedzinowych, zdalnego pulpitu i rozłączyć sesję OpenVPN.
7. **Zalecenia w zakresie bezpieczeństwa informacji i ochrony danych osobowych podczas wykonywania pracy zdalnej**
8. Należy wyodrębnić odpowiednią przestrzeń do pracy tak, aby inne osoby nie miały dostępu do dokumentów, nad którymi pracujemy.
9. Należy zawsze używać haseł dostępowych do systemów informatycznych.
10. Nie należy udostępniać haseł do komputera i systemów informatycznych innym osobom, w tym innym pracownikom oraz członkom rodziny i innym domownikom.
11. Nie należy zapisywać haseł w notatkach, dokumentach elektronicznych
i innych, do których ktoś może mieć dostęp.
12. Nie należy zapisywać haseł w ustawieniach systemowych.
13. Nie należy udostępniać komputera do pracy osobom nieuprawnionym, w tym członkom rodziny i innym domownikom.
14. Należy wylogować się z systemu informatycznego przed odejściem od komputera.
15. Podczas odejścia od wyodrębnionej przez siebie przestrzeni do pracy należy schować dokumenty w taki sposób, aby nie miały do nich dostępu osoby nieupoważnione, w tym członkowie rodziny i inni domownicy.
16. Należy korzystać jedynie z takich narzędzi i aplikacji do pracy zdalnej (w tym wideorozmów), które zostały zaaprobowane przez przełożonego.
17. Programy antywirusowe powinny być uaktywnione przez cały czas pracy każdego komputera.
18. Nie należy otwierać wiadomości mailowych, jeżeli mogą pochodzić
z wątpliwego lub nieznanego źródła.
19. Nie należy otwierać i zapisywać na komputerze plików ani folderów przesłanych drogą elektroniczną, jeżeli mogą pochodzić z wątpliwego lub nieznanego źródła.
20. Nie należy wyłączać, blokować lub odinstalowywać programów zabezpieczających komputer przed szkodliwym oprogramowaniem.
21. Nie należy instalować oprogramowania ani aplikacji o niewiadomym pochodzeniu lub wątpliwej wiarygodności.
22. W przypadku pojawienia się wirusa należy zaprzestać wykonywania jakichkolwiek czynności w systemach informatycznych i powiadomić
o zaistniałej sytuacji przełożonego.
23. Dokumenty zawierające jakiekolwiek dane osobowe, w przypadku gdy nie są już potrzebne, należy zniszczyć w niszczarce po powrocie do siedziby pracodawcy, nie należy wyrzucać ich do kosza.
24. Należy zachować wszelkie środki ostrożności, aby używane urządzenia przenośne (np. dyski, pendrive’y) nie zostały zgubione.
25. Należy korzystać ze służbowej poczty elektronicznej zgodnie z procedurami obowiązującymi u pracodawcy. Jeżeli konieczne jest skorzystanie z prywatnej poczty elektronicznej należy pamiętać o tym, aby pliki były odpowiednio zaszyfrowane. Należy unikać zamieszczania danych osobowych i informacji poufnych w temacie przesyłanej wiadomości.
26. W przypadku przesyłania zaszyfrowanego maila należy pamiętać, aby hasło do odszyfrowania było przesłane innym środkiem komunikacji (np. przesłane smsowo).
27. Przed wysłaniem maila należy upewnić się, że wpisano odpowiedniego adresata.
28. W przypadku jakiegokolwiek naruszenia ochrony danych osobowych należy niezwłocznie powiadomić o tym przełożonego.