

Załącznik nr 6

**Bezpieczeństwo informacji w ramach wykonywania pracy zdalnej
w Uniwersytecie Warmińsko-Mazurskim w Olsztynie**

§ 1 Postanowienia ogólne

1. Niniejszy Załącznik określa zasady ochrony danych osobowych oraz bezpieczeństwa informacji w ramach wykonywania pracy zdalnej.
2. Inspektor Ochrony Danych przeprowadza, w miarę potrzeb – na podstawie zgłoszonego wcześniej przez kierowników jednostek organizacyjnych zapotrzebowania, instruktaż i szkolenie w zakresie ochrony danych osobowych dla pracowników wykonujących pracę zdalną.
3. Pracownik podczas pracy zdalnej może przetwarzać dane osobowe oraz informacje poufne i wewnętrzne wyłącznie w celach związanych z wykonywaniem swoich obowiązków służbowych.
4. Pracownik jest zobowiązany niezwłocznie poinformować swojego bezpośredniego przełożonego w sytuacji, gdy warunki pracy zdalnej mogą naruszać wymogi zawarte w niniejszym Załączniku.
5. Praca zdalna może być wykonywana przez pracownika posiadającego dostęp do służbowego przenośnego sprzętu komputerowego.
6. Praca zdalna wykonywana przez pracownika administracyjnego powinna być świadczona w godzinach pracy Centrum Informatycznego, co zapewni mu pomoc techniczną – niezwłoczną reakcję np. na utratę dostępu do wirtualnej skrzynki uniwersyteckiej pracownika.

§ 2 Rozpoczęcie pracy zdalnej

1. Pracę zdalną może wykonywać wyłącznie pracownik, który odbył szkolenie z zakresu ochrony danych osobowych, uzyskał upoważnienie do ich przetwarzania oraz złożył oświadczenie o zachowaniu w tajemnicy danych osobowych i informacji oraz sposobów ich zabezpieczenia, zgodnie z regulacjami zawartymi w zarządzeniu w sprawie Polityki Bezpieczeństwa Informacji Uniwersytetu Warmińsko-Mazurskiego w Olsztynie (aktualne Zarządzenie Nr 36/2018 Rektora Uniwersytetu Warmińsko-Mazurskiego w Olsztynie z dnia 28 maja 2018 roku w sprawie Polityki Bezpieczeństwa Informacji Uniwersytetu Warmińsko-Mazurskiego w Olsztynie, z późn. zm.).
2. Przed przystąpieniem do wykonywania pracy zdalnej pracownik jest zobowiązany do zapoznania się z niniejszym Załącznikiem, co potwierdza składając stosowne oświadczenie.
3. Oświadczenie, o którym mowa w ust. 2, jest przechowywane w aktach osobowych pracownika, przez okres prowadzenia jego akt przewidziany przepisami prawa pracy.
4. Bezpośredni przełożony prowadzi ewidencję pracowników wykonujących pracę zdalną.

§ 3 Bezpieczeństwo pracy zdalnej

1. Pracownik jest zobowiązany do zabezpieczenia sprzętu służbowego wszelkich nośników informacji i danych osobowych wykorzystywanego w świadczonej pracy zdalnej, w szczególności poprzez:
 - 1) niepozostawianie sprzętu służbowego i wszelkich nośników informacji i danych

- osobowych bez nadzoru;
- 2) niezapisywanie loginu i hasła logowania do systemów teleinformatycznych (dotyczy to zarówno zapisywania fizycznego - np. na kartkach, zapisywania w pamięci przeglądarki) oraz nieudostępnianie ich osobom trzecim;
 - 3) regularną aktualizację oprogramowania na udostępnionych urządzeniach elektronicznych, a także systematyczne skanowanie urządzeń służbowym programem antywirusowym;
 - 4) wykorzystywanie w pracy zabezpieczonej, domowej sieci WiFi (urządzenie sieciowe powinno posiadać aktualne oprogramowanie);
 - 5) niekorzystanie w trakcie pracy zdalnej z publicznych sieci bezprzewodowych;
 - 6) nieudostępnianie osobom trzecim przekazanego przez Uniwersytet sprzętu służbowego oraz innych nośników informacji i danych osobowych, jak również wykorzystywanie go wyłącznie do celów służbowych;
 - 7) zabezpieczenie przekazanego sprzętu hasłem;
 - 8) łączenie się z uniwersyteckimi systemami informatycznymi oraz dyskami sieciowymi, wyłącznie za pośrednictwem sprzętu służbowego i korzystanie z bezpiecznego połączenia za pomocą sieci VPN;
 - 9) każdorazowe upewnienie się, podczas wysyłania wiadomości służbowych, co do poprawności wpisywanych adresatów wiadomości, a w przypadku przesyłania załączników zawierających dane osobowe informacje wewnętrzne lub poufne, zabezpieczenie ich hasłem.
2. Pracownik jest zobowiązany właściwie eksploatować powierzony mu sprzęt oraz utrzymać go w stanie nie gorszym, niż wynika to ze zwykłego zużycia eksploatacyjnego.
 3. Niedozwolone jest gromadzenie, instalowanie i użytkowanie oprogramowania, plików oraz innych informacji pochodzących z nielegalnego lub niewiadomego źródła, jak również niezwiązanych z wykonywaniem obowiązków służbowych pracownika.
 4. Pracownik korzystający ze sprzętu służbowego nie może samodzielnie przekazać go do serwisu zewnętrznego bez zgody kierownika jednostki organizacyjnej, w której jest zatrudniony.

§ 4 Incydenty

Pracownik jest zobowiązany do zgłaszania incydentów bezpieczeństwa informacji i naruszeń ochrony danych osobowych zgodnie z obowiązującymi w tym zakresie przepisami wewnętrznymi.

§ 5 Monitoring korzystania ze sprzętu służbowego

1. Pracownik wykonujący pracę zdalną zobowiązany jest do efektywnego wykonywania powierzonych obowiązków, przestrzegania godzin pracy oraz zasad organizacji czasu pracy. Praca w godzinach nadliczbowych może być świadczona po uzyskaniu uprzedniej zgody bezpośredniego przełożonego.
2. Pracodawca może stosować monitoring techniczny urządzeń służbowych wykorzystywanych do wykonywania pracy zdalnej w celu:
 - 1) potwierdzania obecności pracownika na stanowisku pracy i ewidencjonowania godzin pracy,
 - 2) zapewnienia prawidłowej organizacji pracy,
 - 3) oceny efektywności realizowanych zadań,
 - 4) ochrony informacji poufnych i danych służbowych,
 - 5) zapewnienia właściwego użytkowania udostępnionych pracownikom narzędzi pracy.
3. Monitoring obejmuje wyłącznie okres godzin pracy wskazanych w Regulaminie pracy, w umowie o pracę lub w harmonogramie pracy, świadczonych w trybie zdalnym,

o którym mowa w ust. 1. Monitoring nie może dotyczyć treści prywatnej komunikacji pracownika niezwiązanej z wykonywaniem obowiązków służbowych. Zasady korzystania z urządzeń elektronicznych udostępnionych przez pracodawcę określają odrębne regulacje wewnętrzne obowiązujące w Uniwersytecie. Urządzenia te powinny być wykorzystywane wyłącznie do celów służbowych, z poszanowaniem obowiązujących zasad bezpieczeństwa informacji.

4. Monitoring nie może naruszać prywatności pracownika, w szczególności poprzez rejestrowanie treści prywatnej korespondencji, prywatnych rozmów głosowych czy działań niezwiązanych z wykonywaniem pracy.
5. Przed rozpoczęciem pracy zdalnej (oraz w przypadku zmiany metody prowadzenia monitoringu) pracownik otrzymuje szczegółową informację dotyczącą zakresu prowadzonego monitoringu, w szczególności wykorzystywanego w tym celu programu komputerowego.
6. Dane z monitoringu będą przetwarzane zgodnie z obowiązującymi przepisami o ochronie danych osobowych.
7. Pracodawca może kontrolować przestrzeganie wymogów w zakresie bezpieczeństwa i ochrony informacji, ujętych w niniejszym załączniku.

§ 6 Bezpieczeństwo stanowiska pracy

1. Pracownik powinien przestrzegać następujących zasad przy wykonywaniu pracy zdalnej:
 - 1) przechowywania nośników zawierających dane osobowe oraz informacje wewnętrzne lub poufne w szafkach/pomieszczeniach zamykanych na klucz, uniemożliwiających dostęp do nich przez osoby postronne, m. in. członków rodziny, jak również w sposób zapobiegający ich zniszczeniu przez czynniki środowiskowe (np. zalanie);
 - 2) niepozostawiania nośników zawierających dane osobowe oraz informacje wewnętrzne lub poufne (sprzętu, jak i nośników papierowych) bez nadzoru – zarówno w trakcie wykonywania pracy zdalnej, jak i po jej zakończeniu;
 - 3) blokowania komputera przed każdorazowym opuszczeniem stanowiska do wykonywania pracy zdalnej oraz poprawnego wyłączenia i zabezpieczenia sprzętu po zakończeniu pracy;
 - 4) zabierania dokumentów z drukarek zaraz po ich wydrukowaniu;
 - 5) trwałego niszczenia nieprzydatnych dokumentów, brudnopisów oraz zbędnych kopii, tj. w sposób uniemożliwiający odtworzenie zawartych w nich danych osobowych. Dotyczy to również informacji zapisanych w innej niż papierowa formie – na nośnikach elektronicznych. Jeżeli pracownik nie posiada w domu niszczarki, powinien dokumenty oraz inne nośniki danych np. płyty CD/DVD przechowywać w bezpieczny sposób – uniemożliwiający dostęp do nich przez osoby postronne, a po zakończeniu pracy zdalnej zniszczyć je w Uniwersytecie;
2. Pracownik powinien korzystać z dokumentów papierowych zawierających dane osobowe oraz informacje wewnętrzne lub poufne podczas pracy zdalnej jedynie wyjątkowo, tj. gdy:
 - 1) nie jest możliwe wykonywanie obowiązków wskazanych w inny sposób, np. poprzez bezpieczny dostęp do dokumentów zawierających dane osobowe oraz informacje wewnętrzne lub poufne w formie elektronicznej;
 - 2) nie jest możliwe skorzystanie z dokumentów zanonimizowanych.
3. W celu zminimalizowania ryzyka naruszenia integralności danych oraz utraty ich dostępności, pracownik podczas pracy zdalnej powinien pracować na kopiach dokumentów papierowych zawierających dane osobowe oraz informacje wewnętrzne

lub poufne. Powyższe nie oznacza, że pracownikowi wolno samowolnie wchodzić w posiadanie ww. kopii, np. poprzez ich drukowanie, w szczególności zakazane jest samowolne drukowanie dokumentów zawierających dane osobowe oraz informacje wewnętrzne lub poufne w warunkach domowych. Pracownik musi chronić dane zawarte w kopiach dokumentach tak samo jak w dokumentacji oryginalnej.

4. Pracownik na wyraźne polecenie bezpośredniego przełożonego wykonuje kopie dokumentów niezbędnych do wykonywania czynności służbowych. Po wykonaniu kopii dokumentów pracownik przygotowuje zestawienie określające jakie dokumenty, w jakiej liczbie zostały skopiowane, następnie przekazuje je bezpośredniemu przełożonemu.
5. Wynoszenie dokumentów lub ich kopii powinno mieć miejsce w zabezpieczonej aktówce w taki sposób, aby były niewidoczne dla osób trzecich i zabezpieczone przed ich zniszczeniem, uszkodzeniem lub utratą.
6. Po zakończeniu wykonywania pracy zdalnej pracownik jest zobowiązany do uporządkowania swojego stanowiska pracy oraz wykonania czynności zabezpieczających, adekwatnych do warunków technicznych i lokalowych, polegających na:
 - 1) zabezpieczeniu dokumentacji i pieczętek służbowych;
 - 2) zabezpieczeniu komputerów i nośników informacji;
 - 3) zamknięciu okien i drzwi na klucz.