Załącznik nr 12 do Regulaminu

Procedura ochrony danych osobowych

Procedura Ochrony Danych Osobowych oraz innych danych podlegających ochronie prawnej podczas pracy poza siedzibą Uczelni

§ 1

Wprowadzenie

1. W przypadku świadczenia pracy w formie zdalnej, pracownik zobowiązany jest do przestrzegania wewnętrznych regulacji dotyczących przetwarzania danych osobowych w szczególności Polityki Ochrony Danych Osobowych oraz Regulaminu Ochrony Danych osobowych. Zapisy zawarte w procedurze nie zwalniają z obowiązku przestrzegania pozostałych przepisów prawa oraz wewnętrznych regulacji obowiązujących w Uczelni.
2. Pracownik, którego wniosek o pracę zdalną został rozpatrzony pozytywnie zobowiązany jest do pisemnego potwierdzenia przestrzegania zawartych w dokumencie procedur.

§ 2

Zabezpieczenia organizacyjne podczas pracy zdalnej

1. Praca zdalna wykonywana jest w godzinach pracy wskazanych przez pracownika w oświadczeniu o czasie pracy.
2. Pracownik wykonujący obowiązki zdalnie zobowiązany jest do zabezpieczenia dostępu do urządzeń służbowych przed osobami trzecimi w tym domownikami. W szczególności dotyczy to komputerów przenośnych, telefonów służbowych, drukarek itp.
3. W uzasadnionych przypadkach, w celu wykonywania pracy, pracownik może korzystać z prywatnego komputera po uzyskaniu uprzedniej zgody pracodawcy. W takim przypadku pracownik odpowiada za zapewnienie poufności danych znajdujących się na dysku urządzenia. Sposób wykorzystania sprzętu prywatnego oraz minimalne wymagania techniczne muszą być zatwierdzone przez Sekcję IT. Praca z użyciem prywatnego komputera jest dopuszczalna tylko w wyjątkowych sytuacjach. Podstawowe wymagania techniczne dla prywatnego komputera wykorzystywanego do pracy zdalnej:
   1) system operacyjny Windows 10 lub 11 z zainstalowanymi aktualizacjami krytycznymi (z uwagi na brak wsparcia technicznego dla systemów operacyjnych Windows 7, Windows XP oraz starszych, Pracodawca nie dopuszcza użycia komputerów z powyższymi systemami operacyjnymi),

2) licencjonowany program antywirusowy z automatyczną aktualizacją baz wirusów uruchamiany podczas startu sytemu operacyjnego oraz działający w tle,
3) licencjonowany pakiet Office,
4) silne, minimum ośmioznakowe hasło do konta użytkownika zawierające cyfry, liczby oraz znaki specjalne znane wyłącznie osobie wykonującej pracę zdalną.
5) zaufany dostęp do sieci z wyłączeniem dostępu do sieci otwartych nie wymagających uwierzytelnienia.

4. Do pracy zdalnej na prywatnym komputerze pracodawca nie zapewnia licencjonowanego oprogramowania.
5. W przypadku konieczności pracy z wykorzystaniem dokumentacji papierowej zawierającej dane osobowe oraz inne dane podlegające ochronie prawnej, pracownik może korzystać wyłącznie z kopii dokumentów. Kopie dokumentów należy wykonać w siedzibie uczelni po uprzednim uzyskaniu pisemnej zgody bezpośredniego przełożonego. Wniosek o zgodę musi zawierać wykaz ilościowo - rodzajowy wnioskowanych dokumentów.
6. Dopuszcza się pracę na dokumentach w wersji elektronicznej. Zgodę na korzystanie z tej formy dokumentów musi wyrazić bezpośredni przełożony pracownika. Dokumenty w wersji elektronicznej można przenosić wyłącznie na nośniku z funkcją szyfrowania lub wyposażonym w czytnik linii papilarnych.
7. Uczelnia zastrzega sobie prawo do przeprowadzenia kontroli przestrzegania procedur ochrony danych osobowych w ustalonym z pracownikiem terminie w miejscu świadczenia pracy zdalnej. Kontrola może być przeprowadzona wyłącznie w godzinach pracy pracownika.

§ 3

Zabezpieczenia techniczne obowiązujące podczas pracy zdalnej

1. Pracę zdalną można wykonywać wyłącznie na komputerach przenośnych udostępnianych przez Pracodawcę oraz prywatnych po wcześniejszym zaopiniowaniu ich przez Sekcję IT.
2. Pracodawca nie udostępnia do pracy zdalnej komputerów stacjonarnych.
3. Zabronione jest dokonywanie modyfikacji, instalacji lub dezinstalacji oprogramowania na udostępnionych komputerach. Uprawniona do tego typu działań jest wyłącznie Sekcja IT.
4. Do pracy zdalnej mogą być wykorzystywane wyłącznie komputery z zaktualizowanym systemem operacyjnym oraz oprogramowaniem antywirusowym.
5. Komputer może być podłączony wyłącznie do zaufanej sieci. Niedopuszczalne jest korzystanie z publicznych sieci dostępowych (otwartych). Zaleca się stosowanie szyfrowanego połączenia VPN.

6. Niedopuszczalne jest wykorzystywanie podczas pracy zdalnej konta lub identyfikatora innego użytkownika. Dozwolona jest praca wyłącznie na własnym koncie lub identyfikatorze.
7. Do przesyłania informacji drogą elektroniczną wykorzystywać można wyłącznie służbowe adresy e-mail w domenie awf.poznan.pl. Zabronione jest wykorzystywanie prywatnych adresów do korespondencji służbowej.
8. Podczas wysyłania wiadomości drogą elektroniczną pracownik zobowiązany jest zwracać szczególną uwagę na poprawność adresu odbiorcy.
9. W przypadku konieczności przesłania drogą elektroniczną plików zawierających dane osobowe lub inne dane podlegające ochronie pracownik zobowiązany jest do zabezpieczenia pliku hasłem. Hasło do pliku należy przekazać odbiorcy innym kanałem np. telefonicznie lub SMS-em.
10. Niedopuszczalne jest uruchamianie plików otrzymanych drogą elektroniczną od nieznanych nadawców, klikanie w linki prowadzące do bliżej nieokreślonych stron.
11. Kopie dokumentów (w formie papierowej) należy przechowywać w bezpiecznym miejscu bez możliwości dostępu osób trzecich w tym domowników a po zakończonej pracy zdalnej pracownik zobowiązany jest do ich przekazania pracodawcy.
12. W przypadku konieczności zniszczenia dokumentów papierowych zabronione jest wyrzucanie ich na śmietnik. Dokumenty tego typu należ zniszczyć w sposób bezpieczny z użyciem niszczarki.
13. Zabronione jest kopiowanie oraz przechowywanie dokumentów zawierających dane osobowe lub inne dane podlegające ochronie z wykorzystaniem prywatnych komputerów oraz nośników zewnętrznych.
14. W sprawach nieuregulowanych procedurą mają zastosowanie odpowiednie przepisy powszechnie obowiązującego prawa oraz przepisy wewnętrzne określające zasady ochrony danych osobowych, obowiązujące w Akademii Wychowania Fizycznego w Poznaniu.