Zarządzenie nr 50

Rektora Zachodniopomorskiego Uniwersytetu Technologicznego w Szczecinie

z dnia 28 kwietnia 2023 r.

w sprawie Wymogów w zakresie bezpieczeństwa i ochrony informacji,
w tym procedury ochrony danych osobowych w trakcie pracy zdalnej

Na podstawie art. 23 ustawy z dnia 20 lipca 2018 r. Prawo o szkolnictwie wyższym i nauce (tekst jedn. Dz. U. z 2023 r. poz. 742) w związku z § 14 ust. 4 Porozumienia w sprawie pracy zdalnej, zawartego pomiędzy Zachodniopomorskim Uniwersytetem Technologicznym a Związkami Zawodowymi w ZUT, które stanowi załącznik do zarządzenia nr 42 Rektora ZUT z dnia 14 kwietnia 2023 r., zarządza się, co następuje:

§ 1.

Określa się Wymogi w zakresie bezpieczeństwa i ochrony informacji, w tym procedurę ochrony danych osobowych w trakcie pracy zdalnej, stanowiące załącznik do niniejszego zarządzenia.

§ 2.

Zarządzenie wchodzi w życie z dniem podpisania.

Rektor

dr hab. inż. Jacek Wróbel, prof. ZUT

Załącznik

do zarządzenia nr 50 Rektora ZUT z dnia 28 kwietnia 2023 r.

Wymogi w zakresie bezpieczeństwa i ochrony informacji, w tym procedurę ochrony danych osobowych w trakcie pracy zdalnej

Postanowienia ogólne

§ 1.

1. Niniejsze Wymogi określają zasady bezpieczeństwa informacji i danych osobowych w trakcie pracy zdalnej.
2. Pracodawca przeprowadza, w miarę potrzeb, instruktaż i szkolenie zakresie bezpieczeństwa i ochrony informacji oraz danych osobowych dla pracowników wykonujących pracę zdalną.
3. Pracownicy podczas pracy zdalnej mogą przetwarzać dane osobowe tylko w celach związanych z wykonywaniem swoich obowiązków służbowych.
4. Pracownik w trakcie pracy zdalnej zobowiązany jest dbać o bezpieczeństwo danych, ich poufność oraz integralność. Na pracowniku ciąży obowiązek dbałości o dobro Uczelni w przypadku postępowania z danymi osobowymi w trakcie pracy zdalnej.
5. Pracownik zobowiązany jest natychmiast powiadomić Uczelniane Centrum Informatyki oraz bezpośredniego przełożonego o jakimkolwiek incydencie związanym z wyciekiem danych, zarówno w formie elektronicznej, jak i papierowej, jak również o kradzieży lub zaginięciu powierzonego mu sprzętu.

Praca z danymi w obiegu elektronicznym

§ 2.

1. Praca zdalna musi odbywać się przy użyciu sprzętu służbowego. Wyjątkiem od tej reguły może być okazjonalna praca zdalna, jeśli nie ma możliwości przekazania pracownikowi komputera służbowego.
2. Pracownik wykonujący pracę zdalną musi stosować się do „Zasad korzystania z infrastruktury informatycznej ZUT”, wprowadzonych zarządzeniem nr 32 Rektora ZUT z dnia 5 czerwca 2019 r. W szczególności dotyczy to zasad korzystania z komputerów prywatnych i służbowych oraz zasad bezpieczeństwa informatycznego.
3. Pracownik odpowiada za zabezpieczenie sprzętu służbowego przed dostępem osób trzecich, a w szczególności domowników i dzieci.

4. Sprzęt prywatny wykorzystywany do pracy zdalnej musi spełniać następujące wymagania:
   a) na komputerze wykorzystywanym do pracy zdalnej powinien być utworzony chroniony hasłem odrębny profil (konto) pracownika, do którego nie będą miały dostępu inne osoby;
   b) system operacyjny musi być aktualny (tzn. wersja oprogramowania powinna być wspierana przez producenta, a wszystkie dostępne uaktualnienia bezpieczeństwa powinny być zainstalowane);
   c) na urządzeniu powinno być zainstalowane oprogramowanie antywirusowe z aktualną bazą definicji wirusów;
   d) hasła do systemów informatycznych ZUT nie powinny być zapamiętywane w przeglądarkach internetowych.
5. W przypadku wykorzystywania sprzętu prywatnego oraz konieczności przetwarzania danych osobowych lub innych danych poufnych praca zdalna może być wykonywana wyłącznie poprzez zdalny dostęp do pulpitu serwera lub komputera znajdującego się na terenie ZUT lub do odpowiednio zabezpieczonego przez UCI serwisu WWW. Dostęp jest realizowany poprzez usługę VPN lub przy użyciu protokołu SSL. Przechowywanie plików z danymi osobowymi lub z danymi poufnymi na dyskach twardych komputerów prywatnych lub na innych nośnikach prywatnych jest zabronione.

§ 3.

Zasady bezpiecznego prowadzania wideokonferencji określa załącznik.

Praca z dokumentami papierowymi

§ 4.

1. Wynoszenie dokumentacji papierowej z siedziby ZUT powinno być ograniczone do niezbędnego minimum. Pracodawca może zezwolić pracownikom na korzystanie z dokumentacji papierowej zawierającej dane osobowe w trakcie pracy zdalnej tylko w wyjątkowych sytuacjach. Generalną zasadą pracy zdalnej jest praca w obiegu elektronicznym.
2. W przypadku konieczności korzystania z dokumentacji papierowej poza siedzibą ZUT, w pierwszej kolejności należy rozważyć wykonanie kopii dokumentacji, na której pracownik będzie pracował. Kopie dokumentów z danymi osobowymi podlegają takiej samej ochronie jak oryginały.
3. Drukowanie dokumentów na potrzeby pracy zdalnej należy ograniczyć do niezbędnego minimum. W przypadku dokumentów zawierających dane osobowe należy w miarę możliwości dokonać anonimizacji danych.
4. Wydawane oryginały dokumentów na potrzeby pracy zdalnej podlegają ewidencji przez przełożonego.

5. Po wykorzystaniu oryginałów dokumentów powinny one zostać niezwłocznie zwrócone. Zwrot dokumentów podlega odnotowaniu w prowadzonej ewidencji.

§ 5.

1. Wynoszenie dokumentów lub ich kopii powinno mieć miejsce w zabezpieczonej aktówce i w taki sposób, aby były niewidocznie dla osób trzecich.
2. Pracownik zobowiązany jest do odpowiedniego zabezpieczenia danych w miejscu wykonywania pracy zdalnej, tj. dokumenty i ich kopie powinny być przechowywane w zamykanych na klucz szufladach biurka lub szafach i dostęp do nich osób nieuprawnionych, w tym dzieci i domowników, należy zabezpieczyć.
3. Po wykorzystaniu kopii dokumentacji powinny one zostać w całości zniszczone przez pracownika. W przypadku nieposiadania przez pracownika niszczarki w miejscu pracy zdalnej, powinien on wykonane kopie zniszczyć niezwłocznie w siedzibie ZUT.
4. Po zakończeniu pracy zdalnej pracownik powinien bezwzględnie przestrzegać zasady czystego biurka.

Załącznik

do Wymogów w zakresie bezpieczeństwa i ochrony informacji,

w tym procedurę ochrony danych osobowych w trakcie pracy zdalnej

Zasady bezpiecznego prowadzenia wideokonferencji

I Przed rozpoczęciem wideokonferencji

1. Zapoznaj się z ogólnymi warunkami użytkowania lub polityką prywatności programu, z którego chcesz skorzystać.
2. Sprawdź, czy Twoje rozmowy będą nagrywane i przechowywane.
3. Zweryfikuj, do jakich celów będą wykorzystywane Twoje dane osobowe.
4. Sprawdź, o jakie uprawnienia do danych jesteś proszony - lista kontaktów, lokalizacja itp.
5. Do zainstalowania aplikacji na komputerze użyj oficjalnej strony aplikacji, z której chcesz korzystać; w przypadku urządzeń mobilnych wybierz oficjalny sklep - Google Play lub App Store.
6. Upewnij się, że osoby postronne nie mają dostępu do Twojego ekranu.
7. Sprawdź, czy aplikacja dysponuje niezbędnymi środkami bezpieczeństwa, takimi jak szyfrowanie.
8. Korzystaj z aplikacji webowych, nie desktopowych.
9. Zabezpiecz sieć Wi-Fi silnym hasłem.
10. Przed udostępnieniem swojego ekranu podczas rozmowy zamknij wszystkie okna, tak aby inni uczestnicy konferencji ich nie zobaczyli.
11. Przy podłączeniu się do telekonferencji korzystaj z kodów dostępu/PIN-ów.
12. Przeskanuj program do telekonferencji systemem antywirusowym.

II W trakcie prowadzenia wideokonferencji

1. Ogranicz ilość podawania danych osobowych - użyj pseudonimu i służbowego adresu e-mail.
2. Użyj innego hasła niż używane przez Ciebie w innych usługach.
3. Nie udostępniaj linków do konferencji w mediach społecznościowych.
4. Włącz, jeśli to możliwe, domyślną ochronę hasłem spotkania on-line.
5. Zarządzaj opcjami udostępniania ekranu.
6. W celu wykonywania rozmów służbowych wykorzystuj dostęp do sieci za pomocą szyfrowanego połączenia VPN.
7. Nie udostępniaj dokumentów służbowych za pomocą czatu, który może być publiczny.
8. Jeżeli to możliwe, korzystaj z opcji zamazywania tła (tak żeby rozmówcy nie widzieli Twojego otoczenia).
9. Korzystaj z opcji "poczekalnia", tak abyś mógł kontrolować osoby uczestniczące w telekonferencji; unikniesz przypadkowych lub niechcianych osób.
10. Logując się do telekonferencji, wyłącz mikrofon i kamerę (włączysz je, jak będzie to potrzebne).

III Po zakończeniu wideokonferencji

1. Wyłącz mikrofon i kamerę.
2. Upewnij się, że zakończyłeś spotkanie on-line i zamknąłeś aplikację.
3. Sprawdź, czy program do telekonferencji nie działa w tle.