„ZATWIERDZAM”

REKTOR
Zachodniopomorskiego Uniwersytetu
Technologicznego w Szczecinie
dr hab. inż. Jacek Wróbel, prof. ZUT

Zachodniopomorski
Uniwersytet
Technologiczny
w Szczecinie

Zatwierdzam i wprowadzam do użytku służbowego:

Wytyczne

w zakresie ochrony danych osobowych podczas pracy zdalnej w Zachodniopomorskim Uniwersytecie Technologicznym w Szczecinie

Inspektor Ochrony Danych

INSPEKTOR OCHRONY DANYCH
Zachodniopomorskim Uniwersytecie Technologicznym
w Szczecinie
mgr Artur Kurek

Szczecin - 2020 r.

1. Postanowienia ogólne.

1) Niniejsze wytyczne określają zasady wykonywania pracy zdalnej w związku z ochroną danych osobowych (RODO),

2) Ilekroć w wytycznych jest mowa o:

Pracy zdalnej – należy przez to rozumieć pracę określoną w umowie o pracę, umowie zlecenia, umowie o współpracy oraz innej umowie cywilnoprawnej łączącej pracownika z ZUT, wykonywaną przez czas oznaczony poza miejscem jej stałego wykonywania,

Pracowniku – należy przez to rozumieć osobę zatrudnioną w oparciu o umowę o pracę oraz inną umowę cywilnoprawną, w tym umowę zlecenia, umowę o współpracy, umowę o dzieło, jeśli realizacja tej umowy wiąże się z wykonywaniem obowiązków na rzecz ZUT,

3) Praca zdalna nie stanowi telepracy, o której mowa w art. 675-6717 Kodeksu pracy (tj. z dnia 16 maja 2019 r., Dz.U. z 2019 r. poz. 1040).

2. Prawa i obowiązki ZUT.

1) ZUT zobowiązuje się do przekazywania pracownikowi zadań do wykonania, udzielania informacji merytorycznych oraz organizowania procesu pracy w sposób umożliwiający pracę zdalną,

2) ZUT ma prawo kontrolować wykonywanie pracy zdalnej oraz żądać od pracownika informacji o jej wynikach.

3. Prawa i obowiązki pracownika.

1) Pracownik wykonuje pracę zdalną w miejscu zamieszkania lub innym miejscu uzgodnionym z ZUT,

2) Pracownik zobowiązany jest do realizacji bieżących zadań przekazywanych przez ZUT w ramach zakresu jego obowiązków, w szczególności z wykorzystaniem środków komunikacji elektronicznej,

3) Pracownik ma prawo do wsparcia technicznego ze strony ZUT,

4) Pracownik zobowiązuje się zorganizować stanowisko do pracy zdalnej w sposób zapewniający bezpieczne i higieniczne warunki pracy.

4. Ochrona informacji i danych osobowych.

1) Pracownik zobowiązuje się do zabezpieczania dostępu do sprzętu służbowego oraz posiadanych danych i informacji (w tym także znajdujących się na nośnikach papierowych) przed osobami postronnymi, w tym wspólnie z nim zamieszkującymi,

2) Wykonywanie pracy w formie zdalnej nie zwalnia pracownika z obowiązku

przestrzegania postanowień polityki ochrony danych osobowych wraz z dokumentami powiązanymi,

3) W sprawach nieuregulowanych niniejszymi wytycznymi zastosowanie znajdą wewnętrzne procedury obowiązujące w ZUT oraz przepisy prawa powszechnie obowiązującego.

5. Urządzenia.

Urządzenia i oprogramowanie przekazane przez ZUT do pracy zdalnej służą do wykonywania obowiązków służbowych. Dlatego też należy postępować zgodnie z przyjętą w organizacji procedurą bezpieczeństwa danych osobowych:

1) Nie instaluj dodatkowych aplikacji i oprogramowania niezgodnych z procedurą bezpieczeństwa,

2) Upewnij się, że wszystkie urządzenia z jakich korzystasz mają niezbędne aktualizacje systemu operacyjnego (IOS lub Android), oprogramowania oraz systemu anty-wirusowego,

3) Zanim przystąpisz do pracy, wydziel sobie odpowiednią przestrzeń, tak aby ewentualne osoby postronne, nie miały dostępu do dokumentów, nad którymi pracujesz. Odchodząc od stanowiska pracy każdorazowo blokuj urządzenie, na którym pracujesz,

4) Zabezpieczaj swój komputer poprzez używanie silnych haseł dostępu oraz wielopoziomowe uwierzytelnianie. Pozwoli to na ograniczenia dostępu do urządzenia, a jednocześnie na ograniczenia ryzyka utraty danych w przypadku kradzieży lub zgubienia urządzenia,

5) Podejmij szczególne środki, aby urządzenia z których korzystasz podczas pracy, szczególnie te wykorzystywane do przenoszenia danych, jak dyski zewnętrzne nie zostały zgubione.

6) Jeśli zgubiłeś urządzenie, na którym pracujesz lub zostało skradzione natychmiast podejmij odpowiednie kroki, aby o ile to możliwie, zdalnie wyczyścić jego pamięć.

6. Konta e-mail.

Postępuj zgodnie z obowiązującymi zasadami w ZUT dotyczącymi korzystania ze służbowej poczty elektronicznej (e-mail):

1) Używaj przede wszystkim służbowych kont email. Jeśli pracujesz przetwarzając dane osobowe i musisz używać prywatnego e-maila, upewnij się, że treść i załączniki są właściwie szyfrowane. Unikaj używania danych osobowych lub poufnych informacji w temacie wiadomości,

2) Przed wysłaniem maila upewnij się, że wysyłasz go do właściwego adresata, zwłaszcza jeśli wiadomość zawiera dane osobowe lub dane wrażliwe.

7. Dostęp do sieci i chmury.

1) Używaj tylko z zaufanego dostępu do sieci lub chmury oraz przestrzegaj wszelkich zasad i procedur organizacyjnych dotyczących logowania i udostępniania danych,

2) Jeśli natomiast nie pracujesz w chmurze lub nie masz dostępu do sieci, zadbaj aby przechowywane dane były w bezpieczny sposób zarchiwizowane.

8. Bezpieczeństwo danych.

1) Na bieżąco aktualizuj systemy operacyjne,

2) Systematycznie aktualizuj programy antywirusowe, antymalware i antyspyware,

3) Regularnie skanuj stacje robocze programami antywirusowymi, antymalware i antyspyware,

4) Pobieraj oprogramowanie wyłącznie ze stron producentów,

5) Nie otwieraj załączników z nieznanych źródeł dostarczanych poprzez korespondencję elektroniczną,

6) Nie zapamiętuj haseł w aplikacjach webowych,

7) Nie zapisuj haseł na kartkach,

8) Nie używaj tych samych haseł w różnych systemach informatycznych,

9) Zabezpieczaj serwery plików oraz inne zasoby sieciowe,

10) Zabezpieczaj sieci bezprzewodowe – Access Point,

11) Dostosuj złożoność haseł odpowiednio do zagrożeń,

12) Unikaj wchodzenia na nieznane czy przypadkowe strony internetowe,

13) Nie loguj się do systemów informatycznych w przypadkowych miejscach z niezaufanych urządzeń lub publicznych niezabezpieczonych sieci Wi-Fi,

14) Wykonuj regularne kopie zapasowe,

15) Korzystaj ze sprawdzonego oprogramowania do szyfrowania e-maili lub nośników danych,

16) Szyfruj dane przesyłane pocztą elektroniczną,

17) Szyfruj dyski twarde w komputerach przenośnych,

18) Przy pracy zdalnej korzystaj z szyfrowanego połączenia VPN,

19) Odchodząc od komputera, blokuj stację komputerową,

20) Nie umieszczaj w komputerze przypadkowo znalezionych nośników USB.