

**ZARZĄDZENIE Nr 6/2023**  
**Dyrektora Gminnego Ośrodka Kultury i Sportu w Golczewie**  
**z dnia 9 maja 2023 r.**

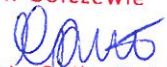
**w sprawie wprowadzenia Podstawowych Zasad Realizacji pracy w formie zdalnej w Gminnym Ośrodku Kultury i Sportu w Golczewie**

Na podstawie art. 67<sup>20</sup> oraz art. 67<sup>26</sup> ustawy z dnia 26 czerwca 1974 r. Kodeks Pracy (Dz. U. z 2022 r. poz. 1510, z późn. zm.), zarządza się, co następuje:

§ 1. Wprowadza się Podstawowe zasady realizacji pracy w formie zdalnej, w brzmieniu określonym w załączniku do niniejszego zarządzenia.

§ 2. Zarządzenie wchodzi w życie z dniem podjęcia.

Dyrektor  
Gminnego Ośrodka Kultury i Sportu  
w Golczewie

  
Dorota Opita-Skubisz



## **PODSTAWOWE ZASADY REALIZACJI PRACY W FORMIE ZDALNEJ**

### **§ 1**

#### **POSTANOWIENIA OGÓLNE**

1. Praca zdalna może być wykonywana przypadku:
  - stanu wyższej konieczności, który to stan wynika z oceny Pracodawcy lub jest wynikiem ustanowionych przepisów prawa lokalnego lub powszechnie obowiązującego;
  - pozytywnie rozpatrzonego przez Pracodawcę wniosku złożonego przez Pracownika, zawierającego uzasadnienie dla udzielenia możliwości realizacji pracy w sposób zdalny.
2. Praca w formie zdalnej jest możliwa wyłącznie w sytuacji, w której umożliwia pracownikowi realizację podstawowych obowiązków wynikających z powierzonego jemu zakresu czynności w czasie, w którym będzie trwała.
3. Z tytułu pracy zdalnej pracownikowi przysługuje zwrot kosztów z tytułu zużycia energii elektrycznej i transferu danych z wykorzystaniem internetu w kwocie 50,00 zł miesięcznie przy założeniu, że okres miesiąca to 22 kolejno następujące po sobie dni robocze. W przypadku pracy w formie zdalnej przez okres krótszy niż określony powyżej, kwota ryczałtu podlegającego wypłacie na rzecz Pracownika, będzie proporcjonalna do ilości faktycznie przepracowanych dni.

### **§ 2**

#### **PRZETWARZANIE INFORMACJI**

1. Niniejsze zasady zostały przygotowane dla potrzeb związanych z ochroną informacji przy wykonywaniu pracy w formie zdalnej i określają podstawowe wymogi obowiązujące Pracownika podczas wykonywania pracy w formule zdalnej.
2. Świadczenie obowiązku pracy w formule zdalnej nie zwalnia pracownika z obowiązku przestrzegania wymogów w zakresie bezpieczeństwa przetwarzania informacji określonych w wewnętrznych dokumentach obowiązujących u Pracodawcy. W związku ze świadczeniem pracy zdalnej Pracownik powinien przestrzegać wewnętrznych dokumentów funkcjonujących u Pracodawcy odnoszących się do przetwarzania danych osobowych, tj. Polityki ochrony danych osobowych, Polityki bezpieczeństwa informacji oraz Instrukcji zarządzania systemem informatycznym. Niniejsze zasady stosuje się jako uzupełnienie ww. aktów wewnętrznych.
3. Pracodawca ma prawo przeprowadzać kontrolę przestrzegania przez Pracownika wymogów w zakresie bezpieczeństwa i ochrony informacji, w tym procedur ochrony danych osobowych, na zasadach określonych w aktach wewnętrznych wymienionych w §1 ust.2 oraz niniejszych zasadach.
4. Pracownik wykonujący pracę zdalną potwierdza w składanym oświadczeniu fakt znajomości aktów wewnętrznych wskazanych w §1 ust.2 oraz niniejszym dokumencie.

### **§ 3**

#### **ZABEZPIECZENIA I OBOWIĄZKI ORGANIZACYJNE]**

1. Pracownik wykonuje pracę zdalną w miejscu zamieszkania lub w innym miejscu uzgodnionym z Pracodawcą.
2. Pracownik zobowiązuje się do dbania o bezpieczeństwo organizacyjne oraz techniczne w związku ze świadczeniem pracy zdalnej, poprzez:

- stworzenie bezpiecznego i ergonomicznego stanowiska pracy,
  - zapewnienie okoliczności, w których lokalizacja stanowiska pracy będzie znajdowała się w tzw. strefie bezpiecznej, do której nie będą miały dostępu osoby trzecie w trakcie realizacji pracy zdalnej,
  - stosowanie zasady „czystego biurka” i „czystego ekranu”,
  - zabezpieczanie po zakończonej pracy przed dostępem powierzonych jemu służbowych urządzeń takich jak komputer, telefon, pendrive, a także nośników papierowych zawierających dane osobowe lub inne informacje klasyfikowane jako chronione przed osobami postronnymi, w tym domownikami,
3. Pracownik zobowiązuje się do zabezpieczania powierzonych urządzeń, o których mowa w §2 ust.2 oraz nośników informacji (niezależnie od ich postaci – papierowe i elektroniczne), zawierających dane osobowe lub inne informacje chronione przed zniszczeniem, utratą, w tym zagubieniem.
  4. Pracownik nie może użytkować sprzętu ani nośników papierowych lub elektronicznych zawierających dane osobowe lub inne informacje poufne Pracodawcy w miejscach publicznych, takich jak: restauracje, bary, parki, centra handlowe, sklepy, parkingi (nawet w zamkniętym pojeździe), środki komunikacji publicznej, biblioteki
  5. W przypadku zmiany warunków lokalowych i technicznych uniemożliwiających wykonywanie pracy zdalnej lub zachowanie warunków określonych w Polityce ochrony danych osobowych i Polityce Bezpieczeństwa Informacji, Pracownik informuje o tym niezwłocznie Pracodawcę.
  6. Pracownik ma prawo do wsparcia technicznego ze strony Pracodawcy. Pracownik niezwłocznie zgłasza Pracodawcy wszelkie uzasadnione potrzeby w tym zakresie.
  7. Pracownik jest zobowiązany korzystać z powierzonego mu przez Pracodawcę Sprzętu wyłącznie w celach służbowych.

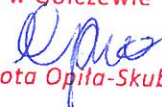
#### **§ 4**

##### **ZABEZPIECZENIA I OBOWIĄZKI TECHNICZNE**

1. Pracownik jest zobowiązany wykonywać pracę zdalną, wykorzystując Sprzęt powierzony mu przez Pracodawcę. Pracownik nie może wykonywać pracy zdalnej, wykorzystując prywatny sprzęt.
2. Pracownik nie może dokonywać modyfikacji w powierzonym Sprzęcie, w szczególności poprzez instalację nowego oprogramowania lub deinstalację oprogramowania już istniejącego.
3. Pracownik zobowiązany jest do używania jedynie zaufanego dostępu do sieci bez możliwości korzystania z otwartych sieci publicznych.
4. Logowanie się do zasobów jednostki należy każdorazowo poprzedzić połączeniem z siecią VPN.
5. Pracownik jest zobowiązany do korzystania ze służbowej skrzynki pocztowej (e-mail) wyłącznie w celach służbowych. Pracownik nie może korzystać z prywatnej skrzynki pocztowej (e-mail) w celach służbowych.
6. Zabrania się kopiowania lub przenoszenia jakichkolwiek danych osobowych przetwarzanych przez Pracodawcę lub innych informacji poufnych Pracodawcy na prywatne komputery, urządzenia mobilne i innego rodzaju sprzęt.
7. Wszystkie informacje, materiały i dokumenty wytworzone lub używane przez Pracownika w ramach pracy zdalnej muszą być przechowywane na serwerze Pracodawcy. Jeżeli Pracodawca przewiduje korzystanie z przechowywania plików w chmurze, Pracownik powinien korzystać z takiego rozwiązania.
8. Jeżeli Pracownik nie pracuje w chmurze ani nie korzysta z dostępu do serwerów Pracodawcy, to jest zobowiązany do zadbania o to, aby przechowywane dane zostały bezpiecznie zarchiwizowane na powierzonym przez Pracodawcę Sprzęcie .

9. Należy dokonywać niezbędnych aktualizacji Sprzętu, systemu operacyjnego lub stosowanych na nich zabezpieczeń wg zaleceń Administratora Systemu Informatycznego.
10. Pracownik zobowiązany jest zwracać szczególną uwagę na poprawność adresu odbiorcy pliku, dokumentu lub innych danych. Przed wysłaniem wiadomości e-mail należy przynajmniej jednokrotnie zweryfikować poprawność adresu. Przy rozsyłaniu korespondencji e-mail wielu adresatom należy używać funkcji UDW, pozwalającej na ukrycie adresów e-mail adresatów.
11. W sytuacji, gdy Pracownik przekazuje za pośrednictwem komunikacji elektronicznej pliki zawierające dane osobowe, powinny one zostać zaszyfrowane odpowiednim oprogramowaniem, a klucz do tych plików powinien zostać przekazany adresatowi inną drogą (np. SMS).
12. Nie należy otwierać podejrzanych załączników lub klikać w nieznane linki przesłane drogą elektroniczną za pośrednictwem maila.
13. Pracownik zobowiązany jest do przestrzegania następujących zasad:
  - stosowania haseł dostępu do Sprzętu. Zabronione jest dezaktywowanie haseł oraz wyłączanie opcji uwierzytelniania dwuskładnikowego tam, gdzie jest ona wymagana przez Pracodawcę,
  - niemodyfikowania konfiguracji dotyczącej ochrony antywirusowej,
  - weryfikacji, czy ewentualne logowanie się do aplikacji odbywa się za pomocą szyfrowanego połączenia SSL/TLS (z kłódką oraz adresem www rozpoczynającego się frazą „https.”).
14. Pracownik jest zobowiązany przestrzegać prawa własności intelektualnej osób trzecich, w tym prawa własności przemysłowej i prawa autorskiego, jak również innych przepisów powszechnie obowiązującego prawa.
15. Pracownik nie ma prawa korzystać ze Sprzętu w celu przeglądania lub rozpowszechniania treści o charakterze obraźliwym, niemoralnym, niestosownym, mając na uwadze powszechnie obowiązujące zasady postępowania.

Dyrektor  
Gminnego Ośrodka Kultury i Sportu  
w Golczewie

  
Dorota Opila-Skubisz

