

**Zarządzenie 72/2020**  
**Rektora Karkonoskiej Państwowej Szkoły Wyższej w Jeleniej Górze z**  
**dnia 6 października 2020 roku**

**w sprawie:** zasad pracy zdalnej w Karkonoskiej Państwowej Szkole Wyższej w Jeleniej Górze.

**Na podstawie:** art. 23 ust. 2 pkt 2, art. 50 ust. 1 i art. 51 ust. 1 ustawy: Prawo o szkolnictwie wyższym i nauce z dnia 20 lipca 2018 r. (t.j Dz.U. z 2020 r., poz. 85), § 14 ust. 2 pkt 6 oraz § 86 ust. 1, zarządzam, co następuje:

**§ 1**

Niniejsze zarządzenie określa zasady wykonywania pracy zdalnej oraz związane z tym prawa i obowiązki pracowników w Karkonoskiej Państwowej Szkole Wyższej w Jeleniej Górze.

1. Ilekroć w zarządzeniu jest mowa o:
  - 1) Pracy zdalnej – należy przez to rozumieć pracę określoną w umowie o pracę, umowie zlecenia, umowie o współpracy oraz innej umowie cywilnoprawnej łączącej Pracownika z Pracodawcą, wykonywaną przez czas oznaczony poza miejscem jej stałego wykonywania, jeżeli wykonywanie pracy poza takim miejscem jest możliwe,
  - 2) Pracownikowi – 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 Karkonoskiej Państwowej Szkoły Wyższej w Jeleniej Górze w miejscu ich stałego wykonywania wyznaczonym przez Pracodawcę.
  - 3) Pracodawcy – Rektor KPSW w Jeleniej Górze
2. Praca zdalna nie stanowi telepracy, o której mowa w art. 675-6717 Kodeksu pracy (t.j. z dnia 16 maja 2019 r., Dz.U. z 2019 r. poz. 1040).

**§ 2**

1. Pracownik jest zobowiązany do świadczenia pracy zdalnej:
  - 1) po złożeniu przez Pracodawcę oświadczenia w formie pisemnej lub elektronicznej dotyczącego polecenia wykonywania pracy zdalnej, którego wzór stanowi załącznik nr 1 do niniejszego zarządzenia.
  - 2) po udzieleniu zgody na pracę zdalną od Pracodawcy lub bezpośredniego przełożonego w związku z wnioskiem pracownika o umożliwienie pracy zdalnej, którego wzór stanowi załącznik nr 2 do niniejszego zarządzenia, jeśli wykonywanie pracy na danym stanowisku umożliwia pracę w innym miejscu niż miejsce stałego jej wykonywania.
2. Wniosek pracownika, o którym jest mowa w ust. 1 pkt 2 składany jest do Pracodawcy za pośrednictwem:
  - 1) właściwego dziekana w przypadku wniosku pracownika będącego nauczycielem akademickim z wyjątkiem prorektora i kanclerza, którzy składają wniosek bezpośrednio do Rektora;
  - 2) bezpośredniego przełożonego w przypadku pracownika niebędącego nauczycielem akademickim.
3. Warunki i zasady pracy zdalnej, w tym zakres i harmonogram wykonywanej pracy określa Pracodawca, jednakże pracownik może także zaproponować własny harmonogram i zakres pracy, który będzie mógł realizować po uzyskaniu zgody Pracodawcy.

4. W przypadku podjęcia pracy zdalnej Pracownika obowiązują zasady pracy zdalnej określone w niniejszym zarządzeniu.
5. Pracownik podejmując pracę zdalną zapewnia odpowiednie warunki świadczenia tej pracy.
6. Jeżeli Pracownik nie ma możliwości świadczenia pracy zdalnej z zapewnieniem właściwych zabezpieczeń, w szczególności ze względu na siłę wyższą (np. brak prądu lub Internetu), niezwłocznie zgłasza to Pracodawcy i postępuje zgodnie z jego instrukcjami.
7. Złamanie zasad pracy zdanej lub niedostosowanie się do postanowień niniejszego rozdziału stanowi naruszenie obowiązków pracowniczych.

### § 3

1. Pracodawca zobowiązuje się do przekazywania Pracownikowi zadań do wykonania, udzielania informacji merytorycznych oraz organizowania procesu pracy w sposób umożliwiający Pracownikowi pracę zdalną, jednakże pracownik może także zaproponować własny harmonogram i zakres pracy, który będzie mógł realizować po uzyskaniu zgody Pracodawcy.
2. Pracodawca ma prawo kontrolować wykonywanie pracy zdalnej oraz żądać od Pracownika informacji o jej wynikach.
3. Pracodawca, jeżeli zajdzie taka potrzeba, może w każdym czasie odwołać Pracownika z pracy zdalnej. Odwołanie Pracownika jest dokonywane w formie pisemnej lub elektronicznej.

### § 4

1. Pracownik, po otrzymaniu decyzji o podjęciu pracy zdalnej, informuje o tym fakcie Dział Kadr i Sekcję Informatyków.
2. Pracownik wykonuje pracę zdalną w miejscu zamieszkania lub innym miejscu uzgodnionym z Pracodawcą. Pracownik jest zobowiązany do wykonywania pracy zgodnie z treścią umowy łączącej go z Pracodawcą oraz zakresem obowiązków.
3. Pracownik zobowiązuje się do:
  - 1) pozostawania dyspozycyjnym dla Pracodawcy w ustalonych godzinach pracy i przyjmowania do realizacji bieżących zadań przekazywanych Pracownikowi w ramach zakresu jego obowiązków, w szczególności z wykorzystaniem środków komunikacji elektronicznej,
  - 2) bieżącego informowania o wynikach swojej pracy oraz przedstawiania wyników swojej pracy Pracodawcy,
  - 3) potwierdzania obecności w pracy poprzez wysłanie wiadomości e-mail do Działu Kadr przed każdym rozpoczęciem pracy zdalnej.
4. Pracownik ma prawo do wsparcia technicznego ze strony Pracodawcy. Pracownik niezwłocznie zgłasza Pracodawcy wszelkie uzasadnione potrzeby w tym zakresie.
5. Pracownik zobowiązuje się zorganizować stanowisko do pracy zdalnej w sposób zapewniający bezpieczne i higieniczne warunki pracy.

### § 5

1. Pracownik musi zapewnić właściwe warunki umożliwiające mu skuteczną pracę zdalną z zachowaniem właściwego poziomu bezpieczeństwa informacji.
2. Niedozwolone jest podejmowanie pracy zdalnej w miejscach publicznych, gdzie osoby postronne mogłyby usłyszeć fragmenty służbowych rozmów lub zapoznać się z fragmentami wykonywanej pracy.

3. Pracując w domu należy zapewnić, aby domownicy nie mieli wglądu w wykonywaną pracę, w szczególności poprzez właściwe ustawienie ekranu komputera, innego urządzenia mobilnego np. smartfona, tableta, a także zapewnienie pracy z dokumentami w sposób uniemożliwiający wgląd.
4. Praca zdalna powinna odbywać się zgodnie z harmonogramem ustalonym z Pracodawcą, co oznacza, że Pracownik jest dostępny i realizuje swoje działania w ustalonych godzinach.
5. Odchodząc od komputera lub kończąc korzystanie z innego urządzenia mobilnego np. smartfona, tableta, należy upewnić się, że urządzenie zostało zablokowane.

## § 6

1. Pracownik wykonuje pracę zdalną z wykorzystaniem urządzeń prywatnych a jeżeli nie ma takiej możliwości, może wystąpić do Pracodawcy o udostępnienie urządzeń służbowych.
2. Jeżeli Pracodawca udostępnia pracownikowi modem Internetowy lub telefon służbowy z dostępem do Internetu, który może pełnić funkcję HotSpot, Pracownik powinien korzystać w pierwszej kolejności z tych urządzeń.
3. W przypadku korzystania z domowej sieci WiFi, należy upewnić się, że została ona skonfigurowana w sposób minimalizujący ryzyko włamania, w szczególności:
  - 1) połączenie WiFi jest szyfrowane z wykorzystaniem standardu co najmniej WPA2 a nawiązanie połączenia z routerem wymaga podania odpowiednio skomplikowanego hasła szyfrującego;
  - 2) hasło powinno składać się z co najmniej 8 znaków, w tym z dużych i małych liter oraz cyfr i znaków specjalnych;
  - 3) jeśli to możliwe, należy zmienić login do panelu administracyjnego routera na własny;
  - 4) dostęp do panelu administracyjnego routera jest możliwy wyłącznie z urządzeń znajdujących się w sieci domowej;
  - 5) został zmieniony domyślny adres routera na inny.
4. Porad i wsparcia w zakresie konfiguracji sieci domowej, w tym jej zabezpieczenia na potrzeby pracy zdalnej udzielają pracownicy Sekcji Informatyków.

## § 7

1. Zabronione jest udostępnianie urządzeń wykorzystywanych do realizowania pracy zdalnej innym osobom, np. domownikom. Jeśli do pracy zdalnej wykorzystywane jest urządzenie prywatne, z którego korzystają inne osoby, należy założyć osobne konto w systemie operacyjnym, zabezpieczone hasłem.
2. Jeżeli praca zdalna wykonywana jest na służbowym sprzęcie, urządzenie to jest przekazywane Pracownikowi protokolarnie na podstawie umowy o odpowiedzialności materialnej za powierzone mienie.
3. Po otrzymaniu zgody na pracę zdalną i uzgodnieniu z pracodawcą z jakich urządzeń będzie korzystał pracownik w celu jej zrealizowania, pracownik niezwłocznie zgłasza ten fakt do Kierownika Sekcji Informatyków.
4. Kierownik Sekcji Informatyków odnotowuje, które urządzenia są wykorzystywane przez Pracownika do pracy zdalnej, jeżeli to niezbędne, pracownicy Sekcji Informatyków przeprowadzają ich przegląd.
5. W przypadku, gdy przegląd jest niemożliwy, pracownik na żądanie pracownika Sekcji Informatyków udostępnia urządzenie zdalnie, w celu dokonania jego zdalnego przeglądu.
6. Minimalne wymagania w zakresie bezpieczeństwa:
  - 1) na urządzeniu jest legalne i aktualne oprogramowanie,

- 2) zostały włączone automatyczne aktualizacje,
  - 3) została włączona zapor systemowa,
  - 4) został zainstalowany i działa w tle program antywirusowy,
  - 5) zalogowanie do systemu operacyjnego wymaga uwierzytelnienia, np. poprzez indywidualny login i hasło użytkownika, kod PIN, token,
  - 6) wyłączono autouzupełnianie i zapamiętywanie hasła w przeglądarce internetowej,
  - 7) został zainstalowany program umożliwiający zaszyfrowanie i odszyfrowanie danych (np. 7-zip),
  - 8) zostało ustawione automatyczne blokowanie urządzenia po dłuższym braku aktywności,
  - 9) jeżeli urządzenie daje taką możliwość, praca jest wykonywana na koncie z ograniczonymi uprawnieniami.
7. Pracodawca może dodatkowo wymagać, aby urządzenie wykorzystywane do pracy zdalnej zawierało inne zabezpieczenia, jak:
- a) zaszyfrowany dysk,
  - b) wyłączone porty pamięci zewnętrznych,
  - c) oprogramowanie służące monitorowaniu wykonywania pracy przez pracownika, wykorzystywane zgodnie z wymaganiami przepisów prawa pracy.

## § 8

1. Do pracy zdalnej Pracownik powinien wykorzystywać tylko i wyłącznie służbowe programy i systemy udostępnione mu przez Pracodawcę.
2. Jeżeli jest niezbędne przesłanie informacji o charakterze poufnym, w szczególności danych osobowych, powinny zostać one zaszyfrowane i zabezpieczone hasłem.
3. Jeżeli informacje poufne będą przekazywane z wykorzystaniem poczty e-mail, powinny zostać udostępnione w zaszyfrowanym i zabezpieczonym hasłem załączniku.
4. Zabezpieczeniu powinny podlegać wszelkiego rodzaju dane osobowe, niezależnie od ich charakteru, nawet jeżeli są to jedynie imiona, nazwiska, czy adresy e-mail.
5. Hasło powinno zostać przekazane odbiorcy inną drogą komunikacji.
6. Hasło powinno być odpowiednio skomplikowane i niesłownikowe.
7. Dozwolone jest ustalenie stałego hasła na komunikację z jednym odbiorcą.
8. Rekomendowane metody zabezpieczania:
  - 1) nadanie hasła do pliku, w którym są dane osobowe;
  - 2) zabezpieczenie pliku lub plików poprzez kompresję z zastosowaniem szyfrowania i zabezpieczeniem archiwum wynikowego hasłem.
9. Każda wiadomość powinna być wysyłana z należytą starannością, polegającą w szczególności na sprawdzeniu, czy jest kierowana do odpowiedniego odbiorcy.
10. W przypadku wysyłania informacji do kilku odbiorców, którzy nie znają się wzajemnie i/lub ich adresy e-mail są adresami prywatnymi, należy skorzystać z opcji Ukrytej kopii.
11. Pracownik może także przekazywać pliki z informacjami chronionymi z wykorzystaniem udostępnionych przez pracodawcę serwerów sieciowych oraz protokołów SCP i SFTP.
12. Wykorzystywanie innych narzędzi do przesyłania i udostępniania plików (weTransfer, Google Drive, DropBoX) może odbywać się tylko za zgodą pracodawcy, po wcześniejszym zaszyfrowaniu i zabezpieczeniu hasłem plików.
13. Ogólne zasady bezpieczeństwa przesyłania, obróbki i przetwarzania danych dotyczą zarówno urządzeń służbowych, jak i prywatnych wykorzystywanych do celów służbowych, z uwzględnieniem ochrony prywatności pracowników.

## **§ 9**

1. Zgodnie z obowiązującym u Pracodawcy zasadami wszystkie dokumenty zawierające informacje poufne, w tym dane osobowe, powinny być przechowywane w szafach zamykanych na klucz w siedzibie Pracodawcy.
2. Obowiązuje ogólny zakaz zabierania dokumentów lub ich kopii poza siedzibę Pracodawcy.
3. Jeżeli do pracy zdalnej niezbędny jest dostęp do dokumentów papierowych, Pracownik zgłasza do pracodawcy prośbę o możliwość ich skopiowania oraz zabrania do domu na czas wykonywania pracy zdalnej.
4. Po otrzymaniu zgody na piśmie lub w formie służbowej wiadomości e-mail, Pracownik może sporządzić kopie niezbędnych dokumentów.
5. Zabronione jest zabieranie poza siedzibę Pracodawcy oryginałów dokumentów.
6. Po skopiowaniu dokumentów pracownik przygotowuje ich zestawienie, zawierające informacje jakie dokumenty, w jakiej liczbie zostały skopiowane.
7. Informacja jest przekazywana do Działu Kadr.
8. Podczas przewożenia dokumentów do miejsca realizowania pracy zdalnej, należy zachować szczególną ostrożność.
9. Praca z dokumentami nie może być wykonywana w miejscu publicznym (świetlica w szkole, kawiarnia, restauracja, galeria handlowa, itp.)
10. Po zakończeniu pracy, wszystkie dokumenty należy zwrócić do Działu Kadr, który weryfikuje ich kompletność.

## **§ 10**

1. Problemy w działaniu udostępnionego sprzętu lub oprogramowania należy niezwłocznie zgłaszać do Sekcji Informatyków.
2. W przypadku zgubienia lub kradzieży sprzętu, dokumentów lub innych nośników informacji, należy niezwłocznie, w tym samym dniu zgłosić zdarzenie Pracodawcy, Kierownikowi Sekcji Informatyków, a także Inspektorowi Ochrony Danych Osobowych.

## **§ 11**

### **Działania niedozwolone**

Niedozwolone jest:

- 1) udostępnianie innym osobom danych służących do uwierzytelnienia do systemów i/lub usług;
- 2) przekazywanie informacji chronionych, w szczególności danych osobowych bez zaszyfrowania i zabezpieczenia hasłem, w szczególności w treści wiadomości e-mail;
- 3) przekazywanie hasła do zabezpieczonych informacji tą samą drogą komunikacji, którą przekazywany jest zaszyfrowany i zabezpieczony hasłem plik lub pliki;
- 4) odmówienie pracownikowi Sekcji Informatyków przeglądu urządzenia;
- 5) niszczenie dokumentów w domu;
- 6) udostępnianie służbowego sprzętu lub sprzętu wykorzystywanego do realizowania zadań służbowych innym osobom;

- 7) dzielenie się informacjami poufnymi z innymi osobami, w szczególności domownikami;
- 8) logowanie się na konto innego użytkownika;
- 9) zabranie dokumentów bez pisemnej lub przekazanej pocztą elektroniczną zgody Pracodawcy;
- 10) zabranie oryginałów dokumentów;
- 11) niezwrócenie dokumentów.

## § 12

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, oraz zniszczeniem.
2. Wykonywanie pracy w formie zdalnej nie zwalnia pracownika z obowiązku przestrzegania postanowień Polityki ochrony danych osobowych przyjętej u Pracodawcy wraz z dokumentami powiązanymi.

## § 13

1. Praca zdalna jest wykonywana przez czas określony w poleceniu Pracodawcy. Pracodawca może dowolnie kształtować okres wykonywania pracy zdalnej.
2. Przed przystąpieniem do wykonywania pracy zdalnej Pracownik zapoznaje z treścią niniejszego zarządzenia, co potwierdza pisemnym lub przekazany pocztą elektroniczną oświadczeniem i zobowiązaniem do jego przestrzegania. Wzór oświadczenia stanowi załącznik nr 3 do zarządzenia.
3. W sprawach nieuregulowanych niniejszym zarządzeniem zastosowanie znajdują wewnętrzne procedury obowiązujące u Pracodawcy oraz przepisy prawa powszechnie obowiązującego.

## § 14

Zarządzenie wchodzi w życie z dniem podjęcia i obowiązuje do dnia wejścia w życie „Regulaminu pracy zdalnej Karkonoskiej Państwowej Szkoły Wyższej w Jeleniej Górze”.

R E K T O R  
dr n. med. *Wioletta Pałczewska*  
prof. KPSW