

Zarządzenie Nr 63/2020
Burmistrza Miasta Świeradów – Zdrój
z dnia 30.09.2020 r.

w sprawie: wprowadzenia rozwiązania organizacyjno-techniczne dotyczącego
wykonywania pracy zdalnej w Urzędzie Miasta Świeradów-Zdrój
na czas zagrożenia epidemicznego lub stanu epidemii

Na podstawie art. 3 ustawy z dnia 2 marca 2020 r. o szczególnych rozwiązaniach związanych z zapobieganiem, przeciwdziałaniem i zwalczaniem COVID-19, innych chorób zakaźnych oraz wywołanych nimi sytuacji kryzysowych (t. j. Dz. U. z 2020 r. Poz. 374 ze zm.) , art. 33 ust. 3 i 5 ustawy z dnia 8 marca 1990 r. o samorządzie gminnym (t.j. Dz. U. z 2020 r. poz. 713 ze zm.), art. 24 i 32 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz. Urz. UE L 119 z 4 maja 2016 r., s. 1, Dz. Urz. UE L127 z dnia 23 maja 2018 r., s. 2) zarządzam, co następuje:

§ 1.

1. W związku z ogłoszeniem zagrożenia epidemicznego lub stanu epidemii na terenie Polski i możliwym potencjalnym zagrożeniem dla zdrowia pracowników Urzędu Miasta Świeradów-Zdrój wirusem SARS-CoV-2 wprowadzam możliwość pracy zdalnej, z wykorzystaniem służbowego lub prywatnego sprzętu komputerowego pracowników Urzędu Miasta Świeradów-Zdrój.
2. Zasady pracy Urzędu w czasie zagrożenia epidemicznego lub stanu epidemii wskazanej w ust. 1 określa Regulamin pracy zdalnej i zasady bezpieczeństwa danych, stanowiący załącznik nr 1 do niniejszego zarządzenia.
3. Decyzję o rozpoczęciu i zakończeniu świadczenia pracy zdalnej podejmuje Burmistrz Miasta wydając pracownikowi na piśmie polecenie pracy zdalnej, wg wzoru stanowiącego załącznik nr 2 do zarządzenia.
4. Wzór ewidencji czasu pracy pracownika, któremu polecono pracę zdalną, stanowi załącznik nr 3 do zarządzenia.

§ 2.

1. Przyjęte rozwiązania organizacyjno-techniczne dotyczące pracy zdalnej obowiązują w czasie określonym tj. do dnia odwołania zagrożenia epidemiologicznego albo stanu epidemii.

§ 3.

1. Zobowiązuję kierujących komórkami organizacyjnymi Urzędu do zapoznania podległych pracowników z przyjętymi rozwiązaniami dotyczącymi pracy zdalnej w Urzędzie, określonymi niniejszym zarządzeniem.
2. Zobowiązuję wszystkich pracowników Urzędu Miasta Świeradów-Zdrój do zapoznania się z treścią i stosowania niniejszego zarządzenia.

§ 4.

Wykonanie zarządzenia powierza się wszystkim kierownikom poszczególnych referatów Urzędu Miasta Świeradów-Zdrój, a w zakresie pracy zdalnej dla osób zatrudnionych na samodzielnych stanowiskach – Burmistrzowi Miasta Świeradów-Zdrój.

§ 5.

Zarządzenie wchodzi w życie z dniem podpisania.

BURMISTRZ

Roland Marciniak

Regulamin pracy zdalnej i zasady bezpieczeństwa danych.

I. Wprowadzenie

1. Niniejszy regulamin określa zasady podejmowania i realizowania pracy zdalnej w związku z ogłoszeniem zagrożenia epidemicznego lub stanu epidemii na terenie Polski i możliwym potencjalnym zagrożeniem dla zdrowia pracowników Urzędu Miasta Świeradów-Zdrój wirusem SARS-CoV-2.
2. Niniejszy dokument opisuje wyjątkowy sposób wykonywania przez pracownika urzędu pracy poza miejscem jej stałego wykonywania, z wykorzystaniem komputera należącego do pracownika lub sprzętu służbowego (w szczególności smartfona) (zwanej dalej „pracą zdalną”).

II. Warunki podjęcia pracy zdalnej. Bezpieczeństwo pracy.

1. Za wyjątkiem zmian wprowadzonych niniejszym zarządzeniem, pracownik zobowiązany jest do pracy zgodnie z warunkami określonymi w:
 - a) w umowie o pracę,
 - b) w informacji do umowy o pracę,
 - c) w zakresie obowiązków,
 - d) zgodnie z oświadczeniami złożonymi znajdującymi się w aktach osobowych,
 - e) w Regulaminie Pracy Urzędu,
 - f) Regulaminie Organizacyjnym Urzędu,
 - g) w Polityce Ochrony Danych Osobowych.
2. O możliwości podjęcia pracy zdalnej przez pracownika decyduje pracodawca.
3. Pracownik może zgłosić pracodawcy chęć podjęcia pracy zdalnej.
4. Warunki i zasady pracy zdalnej określa pracodawca.
5. W przypadku podjęcia pracy zdalnej pracownika obowiązują zasady pracy zdalnej określone w niniejszym Regulaminie.
6. Pracownik podejmując pracę zdalną zapewnia odpowiednie, zgodnie z niniejszym Regulaminem, warunki świadczenia tej pracy. W przypadku świadczenia pracy przy użyciu prywatnego komputera, pracownik zobowiązany jest uzyskać zgodę pracodawcy na pracę z wykorzystaniem tego sprzętu, po uprzednim ustaleniu przez informatyka, czy spełnia on wymogi przewidziane Regulaminem.
7. 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.
8. Pracodawca zobowiązany jest utworzyć pracownikowi wykonującemu pracę zdalną dostęp do służbowej poczty e-mail.
9. Złamanie zasad określonych w Regulaminie lub niedostosowanie się do postanowień niniejszego Regulaminu może stanowić naruszenie obowiązków pracowniczych.

III. Warunki jakie musi spełniać miejsce świadczenia pracy zdalnej

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, jak kawiarnie, restauracje, galerie handlowe, 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 oraz smartfona, 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 ze służbowego smartfona należy upewnić się, że urządzenie zostało zablokowane.

IV. Bezpieczeństwo pracy zdalnej

1. Pracownik wykonuje pracę zdalną z wykorzystaniem urządzeń służbowych, tzn. otrzymanych od pracodawcy albo na komputerze prywatnym.
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.
4. W celu zapewnienia bezpiecznej pracy pracownik zobowiązuje się, w szczególności do:
 - a) zabezpieczenia stacji roboczej poprzez aktualne oprogramowanie antywirusowe,
 - b) posiadanie indywidualnego loginu dostępu do systemu,
 - c) zabezpieczenia komputera hasłem o dużej złożoności hasła konta Administratora komputera i konta użytkownika oraz pracowania na koncie z adekwatnym poziomem uprawnień,
 - d) nieodchodzenia od komputera przed jego uprzednim zablokowaniem,
 - e) nie zapisywania haseł na kartkach w szczególności nie zapisywanie ich w plikach na komputerze prywatnym a także nie udostępniania ich w jakikolwiek sposób innym osobom,
 - f) nieudostępniania sprzętu innym osobom,
 - g) nieinstalowania oprogramowania niebezpiecznego i pochodzącego z niewiadomych źródeł,
 - h) w przypadku konieczności zapisania danych służbowych na komputerze należy przestrzegać zasad bezpiecznego przechowywania danych na komputerze, w tym szyfrowanie danych, i trwałego ich usuwania,
 - i) zadbania o bezpieczeństwo urządzeń w sieci domowej (np. silne hasło do sieci WiFi oraz aktualizacje oprogramowania urządzeń),
 - j) korzystania ze stabilnego i wydajnego łącza internetowego,
 - k) korzystania z bezpiecznych kanałów dostępności do Internetu (np. unikanie „otwartych” kanałów dostępowych WiFi),
 - l) korzystania z aktualnej przeglądarki internetowej. Zalecana jest praca w przeglądarce w tzw. trybie incognito,
 - m) unikania przeglądania stron potencjalnie niebezpiecznych,
 - n) nieużywania prywatnych skrzynek pocztowych czy grup na portalach społecznościowych do komunikacji firmowej,

- o) stosowanie się do wytycznych pracodawcy.

V. Zabezpieczanie przekazywanych informacji

1. Do pracy zdalnej pracownik powinien wykorzystywać tylko i wyłącznie służbowe programy i systemy udostępnione mu przez pracodawcę, w tym służbową skrzynkę pocztową e-mail.
2. Jeżeli jest niezbędne przesłanie informacji o charakterze poufnym, w szczególności danych osobowych, powinny zostać one zabezpieczone i zaszyfrowane hasłem.
3. Jeżeli informacje poufne będą przekazywane z wykorzystaniem poczty e-mail, powinny zostać udostępnione w załączniku zabezpieczonym hasłem.
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 hasłem:
 - a) Nadanie hasła do pliku, w którym są dane osobowe,
 - b) Zabezpieczenie pliku lub plików poprzez kompresję z 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 (UDW/BCC), tzn. adresy wpisać w to pole.
11. Pracownik może także przekazywać pliki z informacjami chronionymi z wykorzystaniem udostępnionych przez pracodawcę serwerów sieciowych lub plików FTP.
12. Wykorzystywanie innych narzędzi do przesyłania i udostępniania plików (weTransfer, Google Drive, DropBoX) może odbywać się tylko za zgodą pracodawcy, po wcześniejszym zabezpieczeniu hasłem plików.

VI. Zasady korzystania z dokumentów w formie papierowej

1. Jeżeli do pracy zdalnej niezbędny jest dostęp do dokumentów papierowych zawierających informacje poufne, w tym dane osobowe, pracownik zgłasza do pracodawcy prośbę o możliwość ich skopiowania oraz zabrania do domu na czas wykonywania pracy zdalnej.
2. Po otrzymaniu zgody na piśmie lub w formie służbowej wiadomości e-mail, pracownik może sporządzić kopie niezbędnych dokumentów.
3. Zabronione jest zabieranie poza siedzibę pracodawcy oryginałów dokumentów.
4. Po skopiowaniu dokumentów pracownik przygotowuje ich zestawienie, zawierające informacje jakie dokumenty, w jakiej liczbie zostały skopiowane.
5. Informacja jest przekazywana pracodawcy.
6. Podczas przewożenia dokumentów do miejsca realizowania pracy zdalnej, należy zachować szczególną ostrożność, aby ich nie zgubić.

7. Praca z dokumentami nie może być wykonywana w miejscu publicznym (świetlica w szkole, kawiarnia, restauracja, galeria handlowa, itp.)
8. Po zakończeniu pracy, wszystkie dokumenty należy zwrócić pracodawcy, który weryfikuje ich kompletność.

VII . Szczególne sytuacje

1. Problemy w działaniu sprzętu lub oprogramowania, wykorzystywanego do pracy zdalnej należy niezwłocznie zgłaszać informatyka.
2. W przypadku zgubienia lub kradzieży sprzętu, dokumentów lub innych nośników informacji, należy niezwłocznie, w dniu zdarzenia zgłosić zdarzenie do pracodawcy, informatyka, a także inspektora ochrony danych.

VIII. Działania niedozwolone

Niedozwolone jest:

- a) Udostępnianie innym osobom danych służących do uwierzytelnienia do systemów i/lub usług,
- b) Przekazywanie informacji chronionych, w szczególności danych osobowych bez zabezpieczenia hasłem, w szczególności w treści wiadomości e-mail,
- c) Przekazywanie hasła do zabezpieczonych informacji tą samą drogą komunikacji, którą przekazywany jest zabezpieczony hasłem plik lub pliki,
- d) Korzystanie z urządzeń, które nie zostały zatwierdzone przez pracodawcę,
- e) Odmówienie informatykowi przeglądu urządzenia,
- f) Niszczenie dokumentów w domu,
- g) Udostępnianie służbowego sprzętu lub sprzętu wykorzystywanego do realizowania zadań służbowych innym osobom,
- h) Dzielenie się informacjami poufnymi z innymi osobami, w szczególności domownikami,
- i) Samodzielne zniszczenie dokumentów w domu,
- j) Logowanie się na konto innego użytkownika,
- k) Zabranie dokumentów bez pisemnej lub elektronicznej zgody pracodawcy,
- l) Zabranie oryginałów dokumentów,
- m) Niezwrócenie dokumentów,
- n) Niepotwierdzenie z pracodawcą zakresu zwróconych danych.

IX. Przepisy końcowe

3. Regulamin ustalony w uzgodnieniu z Zakładową Organizacją Związkową.

Organizacja Zakładowa N8ZZ "Solidarność"
Pracowników Urzędu Miejskiego
ul. Piłsudskiego 5
85-850 Świeradów Zdrój, ul. Piłsudskiego 5
NIP 613-14-72-955, REGON 230326628

A. Mazurek

(związki zawodowe)

BURMISTRZ

Roland Marciniak

(Burmistrz)

Świeradów-Zdrój,r.

.....
(imię i nazwisko pracownika)

.....
(stanowisko)

POLECENIE PRACY ZDALNEJ

Na podstawie art. 3 ustawy z dnia 2 marca 2020 r. o szczególnych rozwiązaniach związanych z zapobieganiem, przeciwdziałaniem i zwalczaniem COVID-19, innych chorób zakaźnych oraz wywołanych nimi sytuacji kryzysowych, w celu przeciwdziałania COVID-19,

polecam Pani/Panu (imię i nazwisko pracownika)
świadczenie pracy, poza miejscem jej stałego wykonywania, tj. w formie pracy zdalnej na
czas zagrożenia wywołanego przez COVID-19 od..... *

.....
(podpis Burmistrza)

* Pracodawca może polecić wykonywanie pracy zdalnej na czas oznaczony (w okresie od.....do.....), jednakże uzasadniony przeciwdziałaniem COVID-19. Pracodawca może skrócić jak i wydłużyć okres świadczenia pracy zdalnej na czas oznaczony, uzasadniony przeciwdziałaniem COVID-19.

Przyjmuję do wiadomości polecenie pracy zdalnej

.....
(data i podpis pracownika)

Praca zdalna – lista obecności, ewidencja czasu pracy

Miesiąc:

Imię i nazwisko pracownika:

Dzień Miesiąca	Godziny pracy od do	Podpis pracownika
1		
2		
3		
4		
5		
6		
7		
8		
9		
10		
11		
12		
13		
14		
15		
16		
17		
18		
19		
20		
21		
22		
23		
24		
25		
26		
27		
28		
29		
30		
31		

.....
(podpis bezpośredniego przełożonego)