GMINA UDANIN
Udanin 26, 55-340 Udanin
Id.390648109, NIP 913-15-00-162

ZARZĄDZENIE Nr 81/2020
Wójta Gminy Udanin
z dnia 30 września 2020 r.

w sprawie przeciwdziałania rozprzestrzenianiu się wirusa SARS–COV-2 wśród pracowników Urzędu Gminy Udanin

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 (Dz.U. z 2020r., poz. 374), zarządzam, co następuje:

§ 1

Zakres przedmiotowy

Niniejsze Zarządzenie określa zasady pracy pracowników Urzędu Gminy Udanin świadczonej poza miejscem jej stałego wykonywania ("praca zdalna").

§ 2

Postanowienia ogólne

1. Zaleca się ograniczenie do minimum bezpośrednich kontaktów pracowników Urzędu Gminy Udanin w miejscu pracy.
2. W celu zapewnienia sprawnej komunikacji zaleca się wykorzystywanie poczty elektronicznej i kontaktów telefonicznych.

§ 3

Warunki dopuszczalności świadczenia pracy zdalnej

1. Wykonywanie pracy zdalnej może zostać polecone, jeżeli pracownik ma umiejętności i możliwości techniczne oraz lokalowe do wykonywania takiej pracy co potwierdza pracownik w oświadczeniu stanowiącym załącznik nr 1 do niniejszego Zarządzenia. W szczególności praca zdalna może być wykonywana przy wykorzystaniu środków bezpośredniego porozumiewania się na odległość.
2. Pracodawca może w każdym czasie cofnąć polecenie wykonywania pracy zdalnej

§ 4

Prawa i obowiązki Pracodawcy

1. Pracodawca jest zobowiązany w szczególności do przekazywania zadań pracownikowi oraz do organizowania procesu pracy w sposób umożliwiający przestrzeganie norm czasu pracy, a ponadto do:
   - dostarczenia pracownikowi sprzętu (komputer, dysk przenośny) oraz jego ubezpieczenia
   - zapewnienia zdalnej pomocy technicznej
2. Pracodawca ma prawo kontrolować wykonywanie pracy zdalnej oraz żądać od pracownika informacji o jej wynikach.

§ 5

Prawa i obowiązki Pracownika

1. Pracownik wykonuje pracę zdalną w miejscu zamieszkania lub innym miejscu uzgodnionym
   z Pracodawcą. Pracownik jest zobowiązany do wykonywania pracy zgodnie z zakresem obowiązków, z uwzględnieniem przepisów prawa pracy oraz Regulaminu pracy.
2. W sytuacjach szczególnych np. opieka nad bliskimi pracownik może wystąpić o zmianę miejsca świadczenia pracy zdalnej. Zgodę na zmianę miejsca świadczenia pracy zdalnej musi wyrazić pracodawca.
3. Ponadto 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 w sposób określony przez Pracodawcę.
   4) ewidencji wykonanych czynności, uwzględniających w szczególności opis tych czynności, a także datę oraz czas ich wykonania
4. Pracownik ma prawo do wsparcia technicznego ze strony Pracodawcy. Pracownik niezwłocznie zgłasza Pracodawcy wszelkie uzasadnione potrzeby w tym zakresie.

§ 6

Zasady postępowania z dokumentami papierowymi wynoszonymi poza obszar przetwarzania Pracodawcy

1. Jeżeli dla realizacji obowiązków służbowych pracownik musi wynieść dokumenty poza obszar przetwarzania zgłasza on ten fakt Przełożonemu. Zgłoszenie może mieć formę pisemną, elektroniczną (e-mail, sms), rozmowa telefoniczna.
2. Pracownik jest zobowiązany do ewidencji pobierania/zdawania każdej dokumentacji niezbędnej do wykonywania pracy zdalnej w zakresie określonym Protokołem zdawczo/odbiorczym stanowiącym załącznik nr 2a i 2b do niniejszego Zarządzenia.
3. Pracownik jest zobowiązany do należytego zabezpieczenia dokumentów w trakcie transportu między siedzibą Pracodawcy a miejscem świadczenia pracy zdalnej w taki sposób aby uniemożliwić zapoznanie się z ich treścią osobom postronnym wykorzystując do tego celu m.in. teczki, koperty
4. Zabrania się otwierania i przeglądania dokumentów w miejscach publicznych
5. Zabrania się pozostawiania dokumentów bez nadzoru np. pozostawienie dokumentów w samochodzie, autobusie.
6. Po dotarciu do miejsca świadczenia pracy zdalnej Pracownik jest zobowiązany do sprawdzenia kompletności pobranej dokumentacji.
7. W przypadku stwierdzenia braków w dokumentacji Pracownik informuje bezpośredniego przełożonego o stanie faktycznym, jeżeli dokumentacja zawierała dane osobowe informuje Inspektora Ochrony Danych Osobowych.

§ 7

Postępowanie z dokumentacją w miejscu wykonywania pracy zdalnej

1. Dokumenty przetwarzane poza siedzibą pracodawcy należy zabezpieczyć przed ich zniszczeniem, uszkodzeniem, dekompletacją, możliwością zapoznania się przez osoby postronne.
2. Po zakończeniu pracy a także w czasie przerwy w pracy dokumenty należy zabezpieczyć tak by nie było one widoczne dla osób postronnych
3. W przypadku stwierdzenia braków w dokumentacji Pracownik informuje bezpośredniego przełożonego o zaistniałym zdarzeniu, jeżeli dokumentacja zawierała dane osobowe informuje Inspektora Ochrony Danych Osobowych.

§ 8

Postępowanie ze sprzętem informatycznym w tym nośnikami danych wykorzystywanych w pracy zdalnej

1. Dopuszcza się używanie służbowych oraz prywatnych urządzeń umożliwiających wykonywanie pracy zdalnej w tym nośników danych umożliwiających ich przenoszenie i archiwizację w tym dyski zewnętrzne, nośniki typu pendrive.
2. Pracownicy pracujący zdalnie są zobowiązani do ewidencjonowania pobierania (wypożyczania) oraz zdawania wszelkich kopii dokumentów, urządzeń, nośników w tym zawierających dane osobowe, które będą przetwarzane poza siedzibą Pracodawcy. Ewidencje w postaci protokołów zdawczo-odbiorczych stanowiących załącznik 2a i 2b do niniejszego Zarządzenia prowadzi pracodawca
3. Do wykorzystania urządzeń i nośników, o których mowa powyżej niezbędna jest zgoda Wójta lub upoważnionego pracownika Urzędu. Zgoda musi być udzielona co najmniej w formie elektronicznej tak by możliwe było jej udokumentowanie na potrzeby zasady rozliczalności
4. Pracownik wykorzystujący prywatne urządzenia do pracy zdalnej zobowiązany jest zapewnić minimalne wymagania w zakresie zapewnienia poufności i integralności dla tych urządzeń określone w Załączniku nr 3b do niniejszego Zarządzenia.
5. W przypadku konieczności przetwarzania na urządzeniach i/lub nośnikach danych, o których mowa w ust. 1 ważnych, poufnych danych w tym danych osobowych konieczne jest stosowanie wobec tych urządzeń i nośników zabezpieczenia kryptograficznego (szyfrowanie)
6. Pracownik, który będzie wykorzystywał urządzenie i/lub nośnik, o którym mowa w ust. 1 zobowiązany jest dostarczyć urządzenie/nośnik do Administratora Systemów Informatycznych/ Informatyka. Za odpowiednie zaszyfrowanie urządzenia/nośnika odpowiedzialny jest ASI.
7. Udostępnione przez Pracodawcę urządzenia i/lub nośniki danych są sprawne technicznie i bezpieczne w momencie przekazania. Pracownik powinien regularnie sprawdzać je pod kątem wszelkich defektów (np. uszkodzeń izolacji, awarii zasilacza), a w przypadku jakichkolwiek wątpliwości dotyczących urządzeń/nośników – skontaktować się z ASI
8. Przy obsłudze urządzeń i/lub nośników danych pracownik zobowiązany jest przestrzegać przepisów bezpieczeństwa i higieny pracy.
9. Po zakończeniu wykonywania pracy zdalnej dane oraz ich kopie przechowywane na przenośnych nośnikach należy przekazać Pracodawcy a następnie przy w obecności ASI trwale je usunąć z nośnika.

§ 9

Bezpieczeństwo i higiena pracy

1. Pracownik zobowiązuje się zorganizować stanowisko do pracy zdalnej w sposób zapewniający bezpieczne i higieniczne warunki pracy
2. Odpowiedzialność Pracodawcy w związku z niezbędnością zapewnienia bezpiecznych i higienicznych warunków pracy ogranicza się do przekazanych środków pracy

§ 10

Czas trwania pracy zdalnej

Czas trwania pracy wykonywanej zdalnie określa się indywidualnie dla każdego pracownika w zależności od okoliczności wprowadzenia pracy zdalnej oraz okresu obowiązywania ww. ustawy.

§ 11

Ochrona danych osobowych, informacji poufnych, tajemnic prawnie chronionych

1. Niniejsze Zarządzenie stanowi udokumentowane polecenie do przetwarzania danych osobowych w zakresie niezbędnym do należytego wykonywania obowiązków w ramach pracy zdalnej
2. Pracownicy Urzędu Gminy Udanin są uprawnieni i zobowiązani do przetwarzania danych osobowych na potrzeby należytego wykonywania obowiązków w ramach pracy zdalnej.
3. Pracownicy są zobowiązani do zachowania w tajemnicy oraz należytego zabezpieczenia danych osobowych, które przetwarzają w związku z wykonywaniem obowiązków w ramach pracy zdalnej.
4. Pracownicy są zobowiązani do ewidencjonowania pobierania (wypożyczania) oraz zdawania wszelkich dokumentów, urządzeń, nośników w tym zawierających dane osobowe, które będą przetwarzane poza siedzibą Administratora Danych Osobowych. Ewidencje w postaci protokołów zdawczo-odbiorczych prowadzi .Sekretarz Gminy w Urzędzie Gminy Udanin.

§ 12

Postanowienia końcowe

1. Decyzje w zakresie nieuregulowanym niniejszym zarządzeniem, podejmuje Urzędu Gminy Udanin.
2. Zarządzenie wchodzi w życie z dniem podpisania i obowiązuje do odwołania, w zależności od rozwoju sytuacji epidemiologicznej i decyzji Rządu RP.

Załącznik nr 1

Oświadczam, że zapoznałem się z treścią Zarządzenia pracy zdalnej w Urzędzie Gminy Udanin i zobowiązuje się do jego przestrzegania.

Posiadam umiejętności i możliwości techniczne oraz lokalowe do wykonywania pracy zdalnej spełniające wymagania Załącznika nr 3b

.....

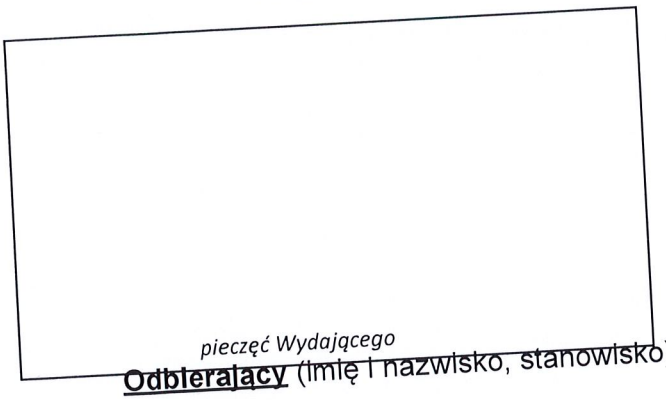
miejscowość, data

.....

podpis pracownika

Załącznik nr 2a

PROTOKÓŁ WYDANIA DOKUMENTÓW/URZĄDZEŃ



pieczęć Wydającego

Odbierający (imię i nazwisko, stanowisko):

.....

Dokumenty podlegające zwrotowi:

1. Wyciągi bankowe za okres od ..... do .....
2. Księgowa dokumentacja źródłowa za okres od ..... do .....
3. Ewidencja sprzedaży I zakupów VAT za okres od .....do.....
4. Ewidencja środków trwałych: pozycje od ..... do .....
5. Ewidencja wyposażenia: pozycje od ..... do .....
6. Inne dokumenty: .....

.....

Urządzenia podlegające zwrotowi

1. Komputer stacjonarny .....
2. Laptop.....
3. Dysk przenośny.....

Odbiorca zobowiązuje się w terminie do ..... tygodni/dni/czasu obowiązywania Zarządzenia lub polecenia służbowego pracy zdalnej w związku z przeciwdziałaniem rozprzestrzenianiu się wirusa SARS–COV-2 wśród pracowników do zwrotu wydanych dokumentów i urządzeń.*

Dokumenty/urządzenia* odebrano dnia: .....

.....

podpis Odbierającego

.....

podpis Wydającego

**niepotrzebne skreślić*

Załącznik nr 2b

PROTOKÓŁ ODBIORU DOKUMENTÓW/URZĄDZEŃ

pieczęć Odbierającego

Odbierający (imię i nazwisko, stanowisko):

.....

Dokumenty podlegające zwrotowi:

7. Wyciągi bankowe za okres od ..... do .....
8. Księgowa dokumentacja źródłowa za okres od ..... do .....
9. Ewidencja sprzedaży I zakupów VAT za okres od .....do..... .....
10. Ewidencja środków trwałych: pozycje od ..... do .....
11. Ewidencja wyposażenia: pozycje od ..... do .....
12. Inne dokumenty: ....

Urządzenia podlegające zwrotowi

4. Komputer stacjonarny .....
5. Laptop.....
6. Dysk przenośny.....

Dokumenty/urządzenia* zdano dnia: .....

Uwagi

.....

....

podpis Zdającego *podpis Odbierającego*

**niepotrzebne skreślić*

Załącznik nr 3a

Wymagania dotyczące bezpiecznej pracy zdalnej z wykorzystaniem systemu informatycznego zapewnionego przez Pracodawcę

1. Wysyłając wiadomości email zawierające dane poufne osobowe i/lub tajemnice prawnie chronione należy zaszyfrować je oraz upewnić się, że wiadomość jest wysyłana do właściwego adresata. Hasło do adresata wiadomości prześlij innym kanałem np. smsem, telefonicznie.
2. Nie należy otwierać załączników lub linków od nieznanych nadawców wiadomości email.
3. Należy korzystać tylko z legalnego oprogramowania.
4. Dysk twardy laptopa służącego do pracy zdalnej, na którym przetwarzane są dane poufne i lub osobowe powinien być zaszyfrowany np. programem Bitlocker, VeraCrypt, ESET Endpoint Encryption lub innym.
5. Dysk zewnętrzny (w tym pendrive) służący do przenoszenia danych poufnych i/lub osobowych powinien być zaszyfrowany oraz przechowywany w sposób zapewniający poufność i integralność danych.
6. W razie konieczności połączenia zdalnego z serwerem Pracodawcy należy wykorzystać metody chronionej transmisji danych np. aplikacja kliencka VPN, w przypadku połączenia serwerem plików poprzez połączenie SFTP (aplikacja kliencka FPT). W przypadku aplikacji chmurowych – tylko z wykorzystaniem protokołu https.
7. Twórz cyklicznie pełne lub przyrostowe kopie bezpieczeństwa danych przetwarzanych w systemie informatycznym. Sprawdzaj ich przydatność do odtworzenia.
8. Stosuj zasady: czystego biurka, ekranu (aktywuj wygaszacz ekranu), wydruku (odbieraj wydruk niezwłocznie po jego wykonaniu).

Pozostałe wymogi dotyczące zachowania bezpieczeństwa informacji w pracy zdalnej

1. Pracuj na skanach, zdjęciach lub kopiach dokumentów, unikaj wynoszenia poza obszar przetwarzania oryginałów dokumentów.
2. Dokumenty lub kopie dokumentów przechowuj w sposób uniemożliwiający utratę; poufności, dostępności, integralności danych.
3. Zbędne kopie dokumentów niszcz w niszczarce lub przechowuj do czasu gdy będzie możliwe ich zniszczenie w niszczarkach Pracodawcy.
4. Pracownicy pracujący zdalnie są zobowiązani do ewidencjonowania pobierania (wypożyczania) oraz zdawania wszelkich kopii dokumentów, urządzeń, nośników w tym zawierających dane osobowe, które będą przetwarzane poza siedzibą Pracodawcy. Ewidencje w postaci protokołów zdawczo-odbiorczych prowadzi pracodawca.

Załącznik nr 3b

Ogólne wymagania jakie musi spełnić prywatny sprzęt informatyczny w celu wykorzystania go w pracy zdalnej

1. Hasło do routera stacjonarnego lub mobilnego wykorzystywanego do pracy zdalnej musi spełniać wymogi Instrukcji Zarządzania Systemem Informatycznym tj. składać się co najmniej z 8 znaków, w którym jest co najmniej duża i mała litera, cyfra i znak specjalny.
2. Komputer prywatny wykorzystywany do pracy zdalnej musi posiadać wyodrębnione konto identyfikujące i uwierzytelniające pracownika za pomocą hasła spełniającego wymogi Instrukcji Zarządzania Systemem Informatycznym tj. składa się co najmniej z 8 znaków, w którym jest co najmniej duża i mała litera, cyfra i znak specjalny zmieniane co 30 dni.
3. Prywatne konto poczty e-mail musi być zabezpieczone hasłem składającym się co najmniej z 8 znaków, w którym jest co najmniej duża i mała litera, cyfra i znak specjalny zmieniane co 30 dni.
4. Wysyłając wiadomości e-mail zawierające dane poufne osobowe i/lub tajemnice prawnie chronione należy zaszyfrować je oraz upewnić się, że wiadomość jest wysyłana do właściwego adresata. Hasło do adresata wiadomości prześlij innym kanałem np. smsem, telefonicznie.
5. Nie należy otwierać załączników lub linków od nieznanych nadawców wiadomości e-mail.
6. Należy zapewnić poufność, integralność plików wykorzystywanych do pracy zdalnej poprzez ich zaszyfrowanie w wyodrębnionych folderach.
7. Należy sprawdzić czy komputer wykorzystywany do pracy zdalnej posiada aktualizacje systemu operacyjnego oraz programu antywirusowego.
8. Należy sprawdzić czy oprogramowanie przeglądarki internetowej posiada zainstalowane aktualizacje.
9. Należy korzystać tylko z legalnego oprogramowania.
10. Dysk twardy laptopa służącego do pracy zdalnej, na którym przetwarzane są dane poufne i lub osobowe powinien być zaszyfrowany np. programem Bitlocker, VeraCrypt, ESET Endpoint Encryption lub innym.
11. Dysk zewnętrzny (w tym pendrive) służący do przenoszenia danych poufnych i/lub osobowych powinien być zaszyfrowany oraz przechowywany w sposób zapewniający poufność i integralność danych.
12. W razie konieczności połączenia zdalnego z serwerem Pracodawcy należy wykorzystać metody chronionej transmisji danych np. aplikacja kliencka VPN, w przypadku połączenia serwerem poprzez połączenie SFTP (aplikacja kliencka FPT). W przypadku aplikacji chmurowych – tylko z wykorzystaniem protokołu https.
13. Twórz cyklicznie pełne lub przyrostowe kopie bezpieczeństwa danych przetwarzanych w systemie informatycznym. Sprawdzaj ich przydatność do odtworzenia.
14. Stosuj zasady: czystego biurka, ekranu (aktywuj wygaszacz ekranu), wydruku (odbieraj wydruk niezwłocznie po jego wykonaniu).

Pozostałe wymogi dotyczące zachowania bezpieczeństwa informacji w pracy zdalnej

1. Pracuj na skanach, zdjęciach lub kopiach dokumentów, unikaj wynoszenia poza obszar przetwarzania oryginałów dokumentów.

2. Dokumenty lub kopie dokumentów przechowuj w sposób uniemożliwiający utratę; poufności, dostępności, integralności danych.
3. Zbędne kopie dokumentów niszcz w niszczarce lub przechowuj do czasu gdy będzie możliwe ich zniszczenie w niszczarkach Pracodawcy.
4. Pracownicy pracujący zdalnie są zobowiązani do ewidencjonowania pobierania (wypożyczania) oraz zdawania wszelkich kopii dokumentów, urządzeń, nośników w tym zawierających dane osobowe, które będą przetwarzane poza siedzibą Pracodawcy. Ewidencje w postaci protokołów zdawczo-odbiorczych prowadzi pracodawca.

Uzasadnienie

Konieczność wprowadzenia tzw. Kodeksu pracy zdalnej wynika z przeprowadzonej wcześniej analizy ryzyka i oceny skutków pracy zdalnej oraz dokumentacji BHP i wprowadzonych procedur COVIdowych na wypadek konieczności powrotu do pracy zdalnej.

WÓJT
Wojciech Płaziuk

Czynność	**Imię i nazwisko oraz funkcja**	**Podpis**
Przygotowanie	Tomasz Więckowski – Inspektor Ochrony Danych	
Weryfikacja pod względem zgodności z prawem	Radca Prawny	RADCA PRAWNY Katarzyna Zawadzka-Żyła
Akceptacja	Andrzej Bielski –Sekretarz Gminy	