ZARZĄDZENIE NR 283/2021
BURMISTRZA IZBICY KUJAWSKIEJ

z dnia 11 marca 2021 r.

w sprawie Regulaminu pracy zdalnej dla pracowników Urzędu Miejskiego w Izbicy Kujawskiej

Na podstawie art. 31 i art. 33 ust. 3 ustawy z dnia 8 marca 1990 roku o samorządzie gminnym (Dz. U. 2020 poz. 713 ze zm.) oraz art.3 ustawy z dnia 2 marca 2020 roku o szczególnych rozwiązaniach związanych z zapobieganiem, przeciwdziałaniem i zwalczaniem COVID-19, innych chorób zakaźnych oraz wywołanych nimi sytuacjami kryzysowymi (Dz. U. 2020r., poz. 374 z późn. zm.) zarządzam, co następuje:

§ 1. Wprowadzam Regulamin pracy zdalnej w Urzędzie Miejskim w Izbicy Kujawskiej, stanowiący załącznik do niniejszego zarządzenia.

§ 2. Wykonanie zarządzenia powierzam Sekretarzowi Gminy.

§ 3. Zarządzenie obowiązuje do odwołania i wchodzi w życie z dniem podpisania.

Burmistrz
mgr Marek Dorabiała

Załącznik do Zarządzenia Nr 283/2021
Burmistrza Izbicy Kujawskiej
z dnia 11 marca 2021 r.

REGULAMIN PRACY ZDALNEJ
W URZĘDZIE MIEJSKIM W IZBICY KUJAWSKIEJ

Rozdział 1.
Postanowienia ogólne

§ 1. 1. Niniejszy Regulamin określa zasady wykonywania pracy zdalnej oraz związane z tym prawa i obowiązki Urzędu Miejskiego oraz jego Pracowników w związku z przeciwdziałaniem i zapobieganiem rozprzestrzeniania się COVID-19.

2. Ilekroć w Regulaminie jest mowa o:

1) **Regulaminie** - należny przez to rozumieć Regulamin pracy zdalnej w Urzędzie Miejskim w Izbicy Kujawskiej;

2) **Pracodawcy** – należy przez to rozumieć Urząd Miejski w Izbicy Kujawskiej;

3) **Pracowniku** – należy przez to rozumieć osobę zatrudnioną na podstawie umowy o pracę łączącej Pracownika z Pracodawcą, wykonywaną przez czas oznaczony poza miejscem jej stałego wykonywania w związku z przeciwdziałaniem COVID-19, jeżeli wykonywanie pracy poza takim miejscem jest możliwe;

4) **Pracy zdalnej** – należy przez to rozumieć pracę określoną w umowie o pracę.

3. Praca zdalna nie stanowi telepracy, o której mowa w art. 67^5-67^{17} ustawie z dnia 26 czerwca 1974 roku - Kodeks pracy (t.j. Dz. U. 2019 poz. 1040 z późn. zm.).

Rozdział 2.
Warunki podjęcia pracy zdalnej

§ 2. Pracownik jest zobowiązany do świadczenia Pracy zdalnej w związku z przeciwdziałaniem COVID-19 po złożeniu przez Pracodawcę oświadczenia w formie pisemnej dotyczącego polecenia wykonywania Pracy zdalnej, które stanowi załącznik Nr 1 do Regulaminu.

§ 3. 1. Osobą reprezentującą Pracodawcę, która jest odpowiedzialna za współpracę z Pracownikiem wykonującym pracę w formie Pracy zdalnej, jest bezpośredni przełożony Pracownika.

2. Osoba, o której mowa w ust. 1 porozumiewa się z pracownikiem telefonicznie.

3. Inne osoby w tym pracownicy Urzędu, wykorzystują do komunikacji z Pracownikiem drogę elektroniczną lub telefoniczną.

§ 4. Pracownik jest w godzinach pracy zobowiązany do utrzymywania technicznej gotowości do komunikowania się z Pracodawcą.

§ 5. Pracownik ma obowiązek niezwłocznego powiadomienia o jakiejkolwiek awarii lub niesprawności lub obniżeniu sprawności sprzętu, urządzeń lub środków komunikacji bezpośredniego przełożonego oraz informatyka urzędu.

§ 6. Naruszenie zasad określonych w Regulaminie lub niedostosowanie się do postanowień niniejszego Regulaminu może stanowić naruszenie obowiązków pracowniczych.

Rozdział 3.
Warunki jakie musi spełniać miejsce świadczenia pracy zdalnej

§ 7. Pracownik musi zapewnić właściwe warunki umożliwiające mu skuteczną Pracę zdalną z zachowaniem właściwego poziomu bezpieczeństwa informacji.

§ 8. Pracując w domu należy zapewnić, aby domownicy nie mieli wglądu w wykonywaną pracę, w szczególności poprzez właściwe ustawienie ekranu komputera.

§ 9. 1. Warunki i zasady Pracy zdalnej, w tym zakres i harmonogram wykonywanej pracy określa bezpośredni przełożony.

2. Praca zdalna wykonywana jest w godzinach pracy Urzędu.

§ 10. Odchodząc od komputera należy upewnić się, że urządzenie zostało zablokowane.

Rozdział 4.
Bezpieczeństwo Pracy zdalnej
Oddział 1.
Internet

§ 11. 1. Pracownik wykonuje pracę zdalną z wykorzystaniem urządzeń służbowych, tzn. otrzymanych od pracodawcy lub na własnym sprzęcie.

2. Jeżeli pracodawca udostępnia Pracownikowi 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) korzystanie z Internetu powinno wymagać uwierzytelnienia, np. poprzez hasło;

2) hasło dostępu 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.

4. Porad i wsparcia w zakresie konfiguracji sieci domowej, w tym jej zabezpieczenia na potrzeby pracy zdalnej udziela informatyk urzędu.

Oddział 2.
Urządzenia służące do pracy zdalnej

§ 12. Zabronione jest udostępnianie urządzeń służbowych wykorzystywanych do realizowania pracy zdalnej innym osobom, np. domownikom.

§ 13. 1. Praca zdalna powinna być realizowana z wykorzystaniem służbowego sprzętu.

2. Zgoda na pracę zdalną obejmuje zgodę na korzystanie ze służbowego sprzętu poza siedzibą Pracodawcy.

§ 14. Jeżeli z jakiś względów pracownik nie może wykonywać pracy zdalnej z wykorzystaniem służbowego sprzętu, zgłasza to pracodawcy, który może wydać zgodę na pracę z wykorzystaniem prywatnych urządzeń.

§ 15. Urządzenie służbowe jest wydawane pracownikowi przez informatyka urzędu.

§ 16. Informatyk urzędu odnotowuje, które urządzania są wykorzystywane przez pracownika do pracy zdalnej, jeżeli to niezbędne, przeprowadza ich przegląd.

Oddział 3.
Zabezpieczenie przekazywanych informacji

§ 17. Do pracy zdalnej Pracownik powinien wykorzystywać tylko i wyłącznie służbowe programy i systemy udostępnione mu przez Pracodawcę.

§ 18. 1. Jeżeli jest niezbędne przesłanie informacji zawierających dane osobowe, powinny zostać one zabezpieczone hasłem.

2. Jeżeli informacje, o których mowa w ust. 1 będą przekazywane z wykorzystaniem poczty e-mail, powinny zostać udostępnione w załączniku zabezpieczonym hasłem.

3. Zabezpieczeniu powinny podlegać wszelkiego rodzaju dane osobowe, niezależnie od ich charakteru, nawet jeżeli są to jedynie imiona, nazwiska lub adresy e-mail.

§ 19. Każda wiadomość powinna być wysyłana z należytą starannością, polegającą w szczególności na sprawdzeniu, czy jest kierowana do odpowiedniego odbiorcy.

§ 20. Zasady pracy zdalnej – sprzęt służbowy

1. Zadania dla pracodawcy:

1) Pracownik otrzymuje komputer służbowy przygotowany wcześniej przez pion informatyki.

2) W miarę możliwości pracodawca przekazuje pracownikowi służbowy sprzęt dostępowy do Internetu.

3) Nie zezwala się na wynoszenie przez pracowników poza jednostkę żadnych dokumentów.

4) Nie zezwala się na drukowanie oraz skanowane dokumentów w miejscu pracy zdalnej.

5) Pracodawca odbiera od pracownika oświadczenie o zapoznaniu się z zasadami pracy zdalnej oraz stosowaniu się do niniejszych zasad.

6) Zapewnia szkolenie pracownikom z zasad pracy zdalnej i wsparcie pionu informatyki w przypadku problemów lub wątpliwości.

2. Zadania dla pionu informatyki:

1) Przygotuj i skonfiguruj komputer aby logował się tylko do zabezpieczonej i odpowiednio skonfigurowanej sieci VPN.

2) Monitoruj ruch sieciowy pod kątem wystąpienia niepożądanego ruchu.

3) Wyłącz możliwość dostępu do BIOS komputera zabezpieczając go hasłem.

4) Wyłącz w BIOS możliwość boot'owania z innych nośników niż dysk twardy komputera.

5) Zaszyfruj dyski twarde, nośniki danych lub karty pamięci, na których będą dane.

6) Zainstaluj i zaktualizuj program antywirusowy oraz skonfiguruj w taki sposób aby bazy wirusów aktualizowały się samoczynnie.

7) Zaktualizuj system operacyjny na komputerze oraz ustaw aktualizacje automatyczne.

8) Zaktualizuj inne oprogramowanie oraz przeglądarki internetowe, które będą wykorzystywane przez pracownika.

9) Zablokuj możliwość instalacji sprzętu zewnętrznego.

10) Włącz i skonfiguruj firewall aby uniemożliwić podłączenie komputera pracownika do niezabezpieczonych sieci Wi-Fi.

11) Wymuś zakaz instalowania innego oprogramowania, jak tylko dopuszczonego przez Jednostkę.

12) Ustaw pracownikom konta dostępu do komputera bez uprawnień administratora.

13) Ustaw hasło do logowania do komputera zgodne z przyjętą polityką haseł.

14) Ustaw wygaszacz ekranu zabezpieczony hasłem nie dłuższym niż 10 min.

15) W przypadku przekazania przez pracodawcę służbowego punktu dostępowego do Internetu odpowiednio go skonfiguruj (szyfrowana transmisja) i zabezpiecz dostęp hasłem.

16) Wymuś szyfrowanie połączeń z służbową pocztą e-mail.

17) Aktualizuj oprogramowanie serwera poczty e-mail oraz monitoruj ruch na serwerze.

18) W przypadku używania przez pracownika smartfonu do pracy oraz obsługi poczty służbowej odpowiednio go zabezpiecz.

19) W przypadku potrzeby wymiany danych pomiędzy pracownikami załóż wspólny, zabezpieczony katalog mając na uwadze właściwe uprawnienia pracowników.

20) Określ maksymalną wielkość pliku, którą można przesłać na wspólny zasób.

21) W przypadku korzystania z komunikatora internetowego odpowiednio go skonfiguruj, zabezpiecz hasłem, sprawdź czy posiada właściwą ochronę kryptograficzną oraz sprawdzaj aktualizacje dla serwera i klienta.

22) Zabezpiecz alternatywne połączenie z Jednostką o tych samych parametrach i zabezpieczeniach w przypadku problemów z już istniejącym.

23) Przeprowadź szkolenie pracowników w zakresie pracy zdalnej.

3. Zadania dla użytkownika:

1) W miejscu pracy zapewnij sobie przestrzeń, która będzie odpowiednia do tego, aby osoby postronne nie miały dostępu do informacji służbowych.

2) Nie pozostawiaj komputera używanego do pracy zdalnej bez nadzoru, a w przypadku krótkotrwałego opuszczania stanowiska pracy zblokuj komputer.

3) Używaj do logowania się na komputerze haseł zgodnych z polityką haseł przyjętą w Jednostce.

4) Używaj tylko rekomendowanych przez administratora przeglądarek internetowych.

5) Nie zapamiętuj haseł w przeglądarkach internetowych.

6) Nie wykorzystuj komputera do prywatnych celów (np. zakupy, gry, itp.).

7) Nie instaluj żadnego oprogramowania bez uprzedniej akceptacji przez pion informatyki.

8) Nie loguj się komputerem do publicznych sieci Wi-Fi.

9) Łącz się z zasobami Jednostki tylko za pomocą skonfigurowanego przez administratora bezpiecznego łącza VPN.

10) Do celów służbowych korzystaj tylko ze służbowej poczty e-mail.

11) Przed wysłaniem wiadomości upewnij się, że wysyłasz ją do właściwego adresata, szczególnie gdy wysyłasz dane osobowe lub inne istotne informacje.

12) Nie otwieraj wiadomości od nieznanych nadawców, a szczególnie załączników niewiadomego pochodzenia oraz nie klikaj w żadne linki lub odnośniki.

13) W przypadku wykorzystywania do kontaktów komunikatora internetowego nie używaj w tym samym czasie innych narzędzi do komunikacji.

14) W przypadku przesyłania plików lub dokumentów za pomocą poczty e-mail lub komunikatora internetowego zawsze zabezpieczaj je hasłem. Hasło przekaż innym kanałem kontaktowym (np. wiadomością SMS).

15) W przypadku utraty sprzętu natychmiast skontaktuj się z wyznaczoną osobą do kontaktu i zadbaj, jeżeli masz taką możliwość, o zdalne usunięcie danych z urządzenia.

§ 21. Zasady pracy zdalnej – sprzęt prywatny

1. Zadania dla pracodawcy:

1) Prywatny sprzęt pracownika należy odpowiednio skonfigurować i zabezpieczyć.

2) W przypadku braku zgody pracownika na ingerencję w jego prywatny sprzęt można wykonać tylko najprostsze prace takie jak pisanie pism, tworzenie tabel, prezentacji, itp., które następnie będą wysyłane poprzez służbowy e-mail jako zaszyfrowane dokumenty.

3) W miarę możliwości przekaż pracownikowi służbowy sprzęt dostępowy do Internetu.

4) Nie zezwala się na drukowanie oraz skanowane dokumentów w miejscu pracy zdalnej.

5) Nie zezwala się na wynoszenie przez pracowników poza jednostkę żadnych dokumentów.

6) Pracodawca odbiera od pracownika oświadczenie o zapoznaniu się z zasadami pracy zdalnej oraz stosowaniu się do niniejszych zasad.

7) Zapewnia szkolenie pracowników z zasad pracy zdalnej i wsparcie pionu informatyki w przypadku problemów lub wątpliwości.

2. Zadania dla pionu informatyki:

1) W przypadku zgody pracownika na ingerencję w prywatny sprzęt wykonaj tylko najistotniejsze czynności, które nie ingerują w prywatne zasoby pracownika.

2) Sprawdź jaki został zainstalowany system operacyjny na sprzęcie pracownika. W przypadku systemów niewspieranych przez Microsoft skonsultuj z pracodawcą dalszą zasadność zlecenia pracy zdalnej – wykonaj test równowagi (mini analizę ryzyka dla takiej sytuacji).

3) W przypadku realizacji dalszej konfiguracji zaktualizuj system operacyjny na komputerze oraz ustaw aktualizacje automatyczne.

4) Przygotuj i skonfiguruj prywatny komputer pracownika aby logował się tylko do zabezpieczonej i odpowiednio skonfigurowanej sieci VPN.

5) Monitoruj ruch sieciowy pod kątem wystąpienia niepożądanego ruchu.

6) Jeśli uzyskasz zgodę pracownika wyłącz możliwość dostępu do BIOS komputera zabezpieczając go hasłem.

7) Jeśli uzyskasz zgodę pracownika wyłącz w BIOS możliwość boot'owania z innych nośników niż dysk twardy komputera.

8) Zaszyfruj dyski twarde, nośniki danych lub karty pamięci, na których będą gromadzone informacje służbowe.

9) Sprawdź czy został zainstalowany program antywirusowy, a jeśli nie jako niezbędne minimum włącz, zaktualizuj Windows Defender oraz ustaw jego automatyczną aktualizację.

10) Zaktualizuj inne oprogramowanie oraz przeglądarki internetowe, które będą wykorzystywane przez pracownika.

11) Włącz i skonfiguruj firewall aby uniemożliwić podłączenie komputera pracownika do niezabezpieczonych sieci Wi-Fi.

12) Załóż pracownikowi konto dostępu do służbowej części komputera bez uprawnień administratora. Konto to będzie wykorzystywane do pracy zdalnej.

13) Ustaw hasło logowania do konta zgodne z przyjętą polityką haseł.

14) Ustaw wygaszacz ekranu zabezpieczony hasłem nie dłuższym niż 10 min.

15) W przypadku przekazania przez pracodawcę służbowego punktu dostępowego do Internetu odpowiednio go skonfiguruj (szyfrowana transmisja) i zabezpiecz dostęp hasłem.

16) Wymuś szyfrowanie połączeń z służbową pocztą e-mail.

17) Aktualizuj oprogramowanie serwera poczty e-mail oraz monitoruj ruch na serwerze.

18) W przypadku używania przez pracownika smartfonu do pracy oraz obsługi poczty służbowej odpowiednio go zabezpiecz.

19) W przypadku potrzeby wymiany danych pomiędzy pracownikami załóż wspólny, zabezpieczony katalog mając na uwadze właściwe uprawnienia pracowników.

20) Określ maksymalną wielkość pliku, którą można przesłać na wspólny zasób.

21) Ustal zasady oraz punk kontaktowy w przypadku awarii lub innych problemów technicznych.

22) W przypadku korzystania z komunikatora internetowego odpowiednio go skonfiguruj, zabezpiecz hasłem, sprawdź czy posiada właściwą ochronę kryptograficzną oraz sprawdzaj aktualizacje dla serwera i klienta.

23) Zabezpiecz alternatywne połączenie z Jednostką o tych samych parametrach i zabezpieczeniach w przypadku problemów z już istniejącym.

24) Przeskanuj komputer aplikacją antywirusową.

25) Przeprowadź szkolenie pracowników w zakresie pracy zdalnej.

26) W przypadku ingerencji w komputer prywatny pracownika pamiętaj o usunięciu wszystkich wprowadzonych zmian, plików, katalogów oraz punktów dostępowych. (Rekomendowanym rozwiązaniem byłoby sformatowanie dysku oraz przywrócenie ustawień sprzed wprowadzenia zmian).

27) W przypadku braku zgody na ingerencję w prywatny sprzęt pracownika przekaż minimalne wymagania jakie musi spełnić pracownik oraz jego sprzęt.

28) W powyższym przypadku nie zezwalaj na logowanie się pracownika do systemów dziedzinowych Jednostki.

3. Zadania dla użytkownika:

1) W miejscu pracy zapewnij sobie przestrzeń, która będzie odpowiednia do tego, aby osoby postronne nie miały dostępu do informacji służbowych.

2) Nie pozostawiaj komputera używanego do pracy zdalnej bez nadzoru, a w przypadku krótkotrwałego opuszczania stanowiska pracy zblokuj komputer i zabezpiecz dokumenty.

3) Załóż osobny katalog służbowy, w którym będziesz przechowywać dokumenty pracodawcy.

4) Używaj do logowania się na komputerze do katalogu służbowego haseł zgodnych z polityką haseł przyjętą w Jednostce.

5) Używaj tylko rekomendowanych przez administratora przeglądarek internetowych.

6) Nie zapamiętuj haseł w przeglądarkach internetowych.

7) Wykorzystując prywatny sprzęt do swoich celów (np. zakupy, gry, itp.) staraj się zachować daleko idące środki ostrożności.

8) Staraj się nie instalować żadnego oprogramowania bez uprzedniej konsultacji z pionem informatyki.

9) Nie loguj się prywatnym komputerem do publicznych sieci Wi-Fi.

10) Jeśli wyraziłeś zgodę na konfigurację prywatnego sprzętu przez pion informatyki łącz się z zasobami Jednostki tylko za pomocą skonfigurowanego przez administratora bezpiecznego łącza VPN.

11) Jeśli nie wyraziłeś zgody na konfigurację prywatnego sprzętu przez pion informatyki najprawdopodobniej nie będziesz miał dostępu do systemów dziedzinowych Jednostki.

12) Do celów służbowych korzystaj tylko z służbowej poczty e-mail.

13) Przed wysłaniem wiadomości upewnij się, że wysyłasz ją do właściwego adresata, szczególnie gdy wysyłasz dane osobowe lub inne istotne informacje.

14) Nie otwieraj wiadomości od nieznanych nadawców, a szczególnie załączników niewiadomego pochodzenia oraz nie klikaj w żadne linki lub odnośniki.

15) W przypadku wykorzystywania do kontaktów komunikatora internetowego nie używaj w tym samym czasie innych narzędzi do komunikacji.

16) W przypadku przesyłania plików lub dokumentów za pomocą poczty e-mail lub komunikatorów internetowych zawsze zabezpieczaj je hasłem. Hasło przekaż innym kanałem kontaktowym (np. wiadomością SMS).

17) W przypadku braku zgody na ingerencję w ustawienia na komputerze prywatnym przez pion informatyki bezwzględnie usuń wszystkie dokumenty, zapamiętane hasła oraz konta służbowe.

18) W przypadku wyrażonej zgody na wprowadzenie ustawień na komputerze prywatnym przez pion informatyki dopilnuj, aby informatyk przywrócił ustawienia do stanu początkowego.

19) W przypadku utraty sprzętu natychmiast skontaktuj się z wyznaczoną osobą do kontaktu i zadbaj, jeżeli masz taką możliwość, o zdalne usunięcie danych z urządzenia. Zagrożenia, które pojawią się podczas pracy na prywatnym sprzęcie:

20) Problemy z licencjami – w przypadku zainstalowanych na komputerze programów „pirackich" konsekwencje może ponieść także pracodawca. Każda instalacja takiego programu jest przestępstwem.

21) W przypadku braku zgody w ingerencję w sprzęt prywatny, a co za tym idzie właściwą konfigurację, istnieje duże ryzyko niespełnienia zasad bezpieczeństwa przyjętych w Jednostce.

22) Wykorzystywanie sprzętu prywatnego do prywatnych celów (zakupy, aukcje, gry, itp.), co może prowadzić do włamania się do sprzętu.

23) Nieusunięcie danych firmowych z komputera prywatnego może grozić utratą kontroli nad nimi.

24) Ponoszenie kosztów lub ewentualne spory w przypadku uszkodzenia lub awarii prywatnego sprzętu - komputery prywatne nie będą objęte ubezpieczeniem Jednostki.

Rozdział 5.
Działania niedozwolone

§ 22. Niedozwolone jest:

1) udostępnianie innym osobom danych służących do uwierzytelnienia do systemów i/lub usług;
2) przekazywanie informacji chronionych, w szczególności danych osobowych bez zabezpieczenia hasłem, w szczególności w treści wiadomości e-mail;
3) przekazywanie hasła do zabezpieczonych informacji tą samą drogą komunikacji, którą przekazywany jest zabezpieczony hasłem plik lub pliki;
4) korzystanie z urządzeń, które nie zostały zatwierdzone przez Pracodawcę;
5) odmówienie informatykowi urzędu przeglądu urządzenia;
6) udostępnianie służbowego sprzętu lub sprzętu wykorzystywanego do realizowania zadań służbowych innym osobom;
7) dzielenie się informacjami chronionymi z innymi osobami, w szczególności domownikami;
8) logowanie się na konto innego użytkownika.

Rozdział 6.
Postanowienia końcowe

§ 23. Problemy w działaniu udostępnionego sprzętu lub oprogramowania należy niezwłocznie zgłaszać do informatyka urzędu.

§ 24. W przypadku zgubienia lub kradzieży sprzętu lub innych nośników informacji, należy niezwłocznie, w dniu zdarzenia zgłosić zdarzenie do bezpośredniego przełożonego, informatyka urzędu, a także do Inspektora ochrony danych osobowych.

§ 25. Zobowiązuję wszystkich pracowników do zapoznania się z niniejszym Regulaminem. Fakt zapoznania się z Regulaminem potwierdza się w formie oświadczenia, które stanowi załącznik Nr 2 do Regulaminu.

Burmistrz

mgr Marek Dorabiała

Załącznik Nr 1 do Regulaminu Pracy Zdalnej w Urzędzie Miejskim w Izbicy Kujawskiej

POLECENIE PRACY ZDALNEJ

dla Pani/Pana .....

z dnia

…….....

1. Na podstawie art. 3 ustawy z dnia 02.03.2020 r. o szczególnych rozwiązaniach związanych z zapobieganiem, przeciwdziałaniem i zwalczaniem COVID-19, innych chorób zakaźnych oraz wywołanych nimi sytuacji kryzysowych polecam Pani/Panu pracę zdalną poza miejscem stałego wykonywania pracy.

2. Praca zdalna będzie wykonywana za pośrednictwem laptopa/komputera stacjonarnego będącego własnością pracownika/pracodawcy*[wybrać właściwe].

3. Obowiązują Panią/Pana godziny pracy zdalnej takie same jak w przypadku pracy w miejscu stałego wykonywania pracy.

Burmistrz Izbicy Kujawskiej

Załącznik Nr 2 do Regulaminu Pracy Zdalnej w Urzędzie Miejskim w Izbicy Kujawskiej

Oświadczenie

……..

(miejscowość, data)

Pracownik:

……..

(imię i nazwisko)

…….

(stanowisko)

Oświadczenie

Oświadczam, że zapoznałem/am się z Regulaminem Pracy Zdalnej w Urzędzie Miejskim w Izbicy Kujawskiej wprowadzonym Zarządzeniem Nr 283/2021 Burmistrza Izbicy Kujawskiej z dnia 11 marca 2021 r. w sprawie Regulaminu pracy zdalnej dla pracowników Urzędu Miejskiego w Izbicy Kujawskiej.

Jednocześnie zobowiązuję się do przestrzegania przepisów o ochronie danych osobowych, a także dbania o bezpieczne przetwarzanie przeze mnie powierzonych danych, bez dostępu do nich dla osób nieupoważnionych, zgodnie z wewnątrzzakładowymi procedurami oraz w/w Regulaminem.

Ponadto oświadczam, że w przypadku wykorzystania podczas pracy zdalnej swojego prywatnego sprzętu lub sprzętu służbowego biorę pełną odpowiedzialność za dostęp do zasobów sieciowych Urzędu.

……

(data i podpis pracownika)