Zarządzenie Nr 120./32020
Wójta Gminy Jasienica
z dnia 20.. października 2020 r.

w sprawie wprowadzenia Regulaminu pracy zdalnej w Urzędzie Gminy Jasienica

Na podstawie art. 31 i art. 33 ust. 3 ustawy z dnia 8 marca 1990 roku o samorządzie gminnym (Dz.U. 2020 poz. 713) 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. 2020 poz. 374 z późn. zm.) zarządzam, co następuje:

§ 1

W związku z wprowadzeniem pracy zdalnej dla pracowników Urzędu Gminy w Jasienicy wprowadzam Regulamin pracy zdalnej w Urzędzie Gminy Jasienica, stanowiący załącznik nr 1 do niniejszego zarządzenia.

§ 2

Wykonanie zarządzenia powierzam Sekretarzowi Gminy.

§ 3

Zarządzenie wchodzi w życie z dniem podpisania.

WÓJT
mgr inż. Janusz Pierzyna

RADCA PRAWNY
Magdalena Maria Kubica
KtB 414

Załącznik nr 1 do Zarządzenia Nr 120.19.2020
Wójta Gminy Jasienica
z dnia 20. października 2020 r.
w sprawie wprowadzenia Regulaminu pracy zdalnej w Urzędzie Gminy Jasienica

Regulamin pracy zdalnej w Urzędzie Gminy Jasienica

I. Wstęp

1. Niniejszy regulamin określa zasady podejmowania i realizowania pracy zdalnej w Urzędzie Gminy Jasienica.
2. W regulaminie pod określeniem "pracownik" należy rozumieć zarówno osoby zatrudnione w ramach stosunku pracy, jak i współpracowników, na stale wykonujących zadania w ramach umów cywilnoprawnych wymagających dostępu do zasobów sprzętowych i informacyjnych Urzędu. Pod określeniem "pracodawca" należy rozumieć zarówno pracodawcę, jak i zlecającego usługi.

II. Warunki podjęcia pracy zdalnej

1. O możliwości podjęcia pracy zdalnej przez pracownika decyduje pracodawca.
2. Pracownik może zgłosić pracodawcy chęć podjęcia pracy zdalnej.
3. Warunki i zasady pracy zdalnej, w tym zakres i harmonogram wykonywanej pracy określa bezpośredni przełożony, jednakże pracownik może zaproponować własny harmonogram i zakres pracy, który będzie mógł realizować po uzyskaniu zgody bezpośredniego przełożonego.
4. W przypadku podjęcia pracy zdalnej pracownika obowiązują zasady pracy zdalnej określone w niniejszym regulaminie oraz Regulaminie pracy.
5. Pracownik zobowiązany jest przestrzegać i stosować się do obowiązującego u pracodawcy Regulaminu pracy.
6. Pracownik podejmując pracę zdalną zapewnia odpowiednie, zgodnie z niniejszym regulaminem oraz przepisami bhp, warunki świadczenia tej pracy.
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 bezpośredniemu przełożonemu i postępuje zgodnie z jego instrukcjami.
8. Złamanie zasad określonych w regulaminie lub niedostosowanie się do postanowień niniejszego regulaminu stanowi naruszenie obowiązków pracowniczych. W przypadku osób realizujących zadania w oparciu o umowy cywilnoprawne postępowanie niezgodnie z niniejszym regulaminem może oznaczać wykonanie zadania niezgodnie z przedmiotem umowy i z wymaganą przez pracodawcę starannością i skutkować rozwiązaniem umowy, a także przewidzianymi w umowie karami umownymi.

9. Pracownik w związku z podjęciem pracy zdalnej po zapoznaniu się z niniejszym regulaminem podpisuje oświadczenie, które stanowi załącznik nr 1 do niniejszego regulaminu.
10. Pracownik wykonujący pracę zdalną jest zobowiązany do wysłania maila do bezpośredniego przełożonego potwierdzającego rozpoczęcie i zakończenie pracy.
11. Bezpośredni przełożony do 2 – dnia roboczego w miesiącu następnym po zakończonym okresie rozliczeniowym składa informację do kadr o czasie pracy pracownika wykonującego pracę zdalną.
12. Nieobecności pracownik zgłasza zgodnie z obowiązującym Regulaminem pracy. Wnioski urlopowe należy przesłać mailem.
13. Pracownik jest zobowiązany do cotygodniowego sporządzenia raportu z wykonanej pracy, poprzez przesłanie maila z informacją określającą zakres wykonanej pracy, do bezpośredniego przełożonego.
14. Pracownik, którego nieobecność w pracy trwa dłużej niż 5 dni roboczych jest zobowiązany do skonsultowania z bezpośrednim przełożonym możliwości przekazania sprzętu służbowego pracodawcy.

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, a także zapewnienie pracy z dokumentami w sposób uniemożliwiający wgląd.
4. Praca zdalna powinna odbywać się zgodnie z harmonogramem ustalonym z bezpośrednim przełożonym, w godzinach wynikających z Regulaminu pracy lub indywidualnego czasu pracy, co oznacza, że pracownik jest dostępny i realizuje swoje działania w ustalonych godzinach.
5. Odchodząc od komputera należy upewnić się, że urządzenie zostało zablokowane za pomocą klawiszy ctrl+alt+del.

IV. Bezpieczeństwo pracy zdalnej

Urządzenia służące do pracy zdalnej

1. Pracownik wykonuję pracę zdalną z wykorzystaniem urządzeń służbowych, tzn. otrzymanych od pracodawcy.
2. Zabronione jest udostępnianie urządzeń wykorzystywanych do realizowania pracy zdalnej innym osobom, np. domownikom.
3. Praca zdalna powinna być realizowana z wykorzystaniem służbowego sprzętu.

4. Zgoda na pracę zdalną obejmuje zgodę na korzystanie ze służbowego sprzętu poza siedzibą pracodawcy.
5. Należy podjąć wszelkie możliwe środki, aby urządzenia służące do pracy zdalnej zabezpieczyć przed zgubieniem lub kradzieżą. Jeżeli jednak dojdzie do zgubienia lub kradzieży urządzenia fakt ten należy niezwłocznie zgłosić pracodawcy.
6. Po otrzymaniu zgody na pracę zdalną i uzgodnieniu z bezpośrednim przełożonym oraz osobą odpowiedzialną za informatykę, z jakich urządzeń będzie korzystał pracownik, w celu jej zrealizowania, pracownik niezwłocznie zgłasza ten fakt do osób odpowiedzialnych za informatykę w UGJ.
7. Pracownik po podpisaniu protokołu przekazania odbiera od osoby odpowiedzialnej za informatykę sprzęt służbowy.
8. Osoba odpowiedzialna za informatykę w UGJ odnotowuje, jaki sprzęt służbowy jest wykorzystywany przez pracownika do pracy zdalnej, jeżeli to niezbędne, przeprowadza jego przegląd.
9. Minimalne wymagania w zakresie bezpieczeństwa:
   - na urządzeniu jest legalne i aktualne oprogramowanie;
   - zostały włączone automatyczne aktualizacje;
   - została włączona zapora systemowa;
   - został zainstalowany i działa w tle program antywirusowy;
   - zalogowanie do systemu operacyjnego wymaga uwierzytelnienia, np. poprzez indywidualny login i hasło użytkownika, kod PIN, token;
   - wyłączono autouzupełnianie i zapamiętywanie hasła w przeglądarce internetowej;
   - został zainstalowany program umożliwiający zaszyfrowanie i odszyfrowanie danych (np. 7-zip);
   - zostało ustawione automatyczne blokowanie urządzenia po dłuższym braku aktywności;
   - jeżeli urządzenie daje taką możliwość, praca jest wykonywana na koncie z ograniczonymi uprawnieniami;
   - zaszyfrowany dysk.

Internet

1. Pracownik wykonuję pracę zdalną z wykorzystaniem urządzeń służbowych, tzn. otrzymanych od pracodawcy.
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. Dopuszcza się podłączanie otrzymanego od pracodawcy sprzętu służbowego do własnej (domowej) sieci komputerowej z dostępem do Internetu po uprzednim upewnieniu się, że została ona skonfigurowana w sposób minimalizujący ryzyko włamania.
4. Porad i wsparcia w tym zakresie udzielają osoby odpowiedzialne za informatykę.
5. Nie dopuszcza się podłączania otrzymanego od pracodawcy sprzętu służbowego do otwartych, ogólnie dostępnych i nieznanych sieci komputerowych.

Zabezpieczanie przekazywanych informacji

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 zabezpieczone 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. Zabrania się przesyłania mailem informacji zaszyfrowanej razem z hasłem. Hasło powinno zostać przekazane odbiorcy inną drogą komunikacji. Jeżeli jest to niemożliwe wskazuje się aby przesłać hasło w kolejnym e-mailu.
6. Hasło powinno być odpowiednio skomplikowane i niesłownikowe.
7. Dozwolone jest ustalenie stałego hasła na komunikację z jednym odbiorcą.
8. Rekomendowane metody zabezpieczania hasłem:
   - nadanie hasła do pliku, w którym są dane osobowe;
   - 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. Odbierając e-maile dokładnie sprawdź nadawcę e-maila. Nie otwieraj wiadomości od nieznanych „podejrzanych" adresatów. Nie otwieraj załączników oraz nie klikaj w zawarte w treści wiadomości linki. To może być atak phishingowy.
12. Wykorzystywanie innych narzędzi do przesyłania i udostępniania plików (weTransfer, Google Drive, DropBoX) może odbywać się tylko za zgodą bezpośredniego przełożonego, po wcześniejszym zabezpieczeniu hasłem plików.

Zasady korzystania z dokumentów w formie papierowej

1. Zgodnie z obowiązującymi u pracodawcy zasadami wszystkie dokumenty zawierające informacje poufne, w tym dane osobowe, powinny być przechowywane w szafach zamykanych na klucz w obszarze przetwarzania danych.
2. Obowiązuje ogólny zakaz zabierania dokumentów lub ich kopii poza siedzibę pracodawcy.
3. Jeżeli do pracy zdalnej niezbędny jest dostęp do dokumentów papierowych, pracownik tworzy zestawienie zawierające informacje jakie dokumenty, w jakiej liczbie zostaną skopiowane i zgłasza do bezpośredniego przełożonego prośbę o możliwość ich skopiowania oraz zabrania do domu, na czas niezbędny do wykonywania pracy zdalnej.

4. Po otrzymaniu zgody na piśmie lub w formie służbowej wiadomości e-mail, pracownik może sporządzić kopie niezbędnych dokumentów zgodnych z zestawieniem.
5. Zabronione jest zabieranie poza siedzibę pracodawcy oryginałów dokumentów.
6. Podczas przewożenia dokumentów do miejsca realizowania pracy zdalnej, należy zachować szczególną ostrożność, aby ich nie zgubić.
7. Dokumenty należy stosownie zabezpieczyć aby podczas ich przenoszenia nie były widoczne dla osób postronnych.
8. Praca z dokumentami nie może być wykonywana w miejscu publicznym (świetlica w szkole, kawiarnia, restauracja, galeria handlowa, itp.).
9. Podczas pracy z kopiami dokumentów należy je zabezpieczyć przed dostępem domowników, współlokatorów itp.
10. Po zakończeniu pracy, wszystkie dokumenty należy zwrócić bezpośredniemu przełożonemu, który weryfikuje ich kompletność zgodnie z zestawieniem.
11. Bezpośredni przełożony po potwierdzeniu kompletności dokumentów przekazuje je pracownikowi w celu zniszczenia. Skopiowane dokumenty należy zniszczyć w niszczarce znajdującej się w Urzędzie Gminy Jasienica.
12. W przypadku zgubienia lub kradzieży dokumentów należy niezwłocznie zgłosić ten fakt bezpośredniemu przełożonemu oraz inspektowi ochrony danych.

V. Szczególne sytuacje

1. Problemy w działaniu udostępnionego sprzętu lub oprogramowania należy niezwłocznie zgłaszać do osób odpowiedzialnych za informatykę w UGJ.
2. W przypadku zgubienia lub kradzieży sprzętu, dokumentów lub innych nośników informacji, należy niezwłocznie, w dniu zdarzenia zgłosić zdarzenie do bezpośredniego przełożonego, osoby odpowiedzialnej za informatykę w UGJ, a także inspektora ochrony danych.

VI. Działania niedozwolone

1. 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, chyba że nie ma innej możliwości;
    d. korzystanie do pracy zdalnej z urządzeń (sprzętu), które nie zostały zatwierdzone przez osobę odpowiedzialną z informatykę w UGJ;
    e. niszczenie dokumentów w domu;
    f. udostępnianie służbowego sprzętu lub sprzętu wykorzystywanego do realizowania

zadań służbowych innym osobom;

g. dzielenie się informacjami poufnymi z innymi osobami;
h. logowanie się na konto innego użytkownika;
i. zabranie dokumentów bez pisemnej lub elektronicznej zgody bezpośredniego przełożonego;
j. zabranie oryginałów dokumentów;
k. niezwrócenie skopiowanych dokumentów;
l. niepotwierdzenie z bezpośrednim przełożonym zakresu zwróconych danych.

WÓJT
mgr inż. Janusz Pierzyna

OŚWIADCZENIE,
w związku z podjęciem pracy zdalnej

Ja niżej podpisany/a ..... oświadczam, że w związku z podjęciem pracy zdalnej zostałem/am zapoznana/y z Regulaminem pracy zdalnej w Urzędzie Gminy Jasienica i mam świadomość że:

1. Do przetwarzania danych osobowych Pracodawcy dopuszczeni są wyłącznie upoważnieni pracownicy Urzędu Gminy Jasienica a przekazany sprzęt służbowy służy tylko i wyłącznie do wykonywania zadań służbowych i nie będę z niego korzystać w innych celach niż tych związanych z pracą.
2. W związku z podjęciem pracy zdalnej jestem zobowiązana/y do przestrzegania zapisów zawartych w Regulaminie pracy zdalnej w Urzędzie Gminy Jasienica, w szczególności poprzez:
    a. nadzór i zabezpieczenie przekazanego sprzętu przed zgubieniem i kradzieżą;
    b. odpowiednie przystosowanie miejsca świadczenia pracy zdalnej;
    c. przestrzeganie wytycznych dotyczących bezpieczeństwa pracy zdalnej;
    d. odpowiednie zabezpieczanie przekazywanych informacji;
    e. przestrzeganie zasad korzystania z dokumentów w formie papierowej;
3. W przypadku zgubienia lub kradzieży sprzętu, dokumentów lub innych nośników informacji niezwłocznie, w dniu zdarzenia zgłoszę zdarzenie bezpośredniemu przełożonemu, osobie odpowiedzialnej za informatykę w UGJ, a także inspektorowi ochrony danych.
4. Mam świadomość jakie działania w związku z podjęciem pracy zdalnej są niedozwolone.
5. Przyjmuję do wiadomości, iż postępowanie sprzeczne z powyższymi zobowiązaniami może być uznane za naruszenie obowiązków pracowniczych w rozumieniu Kodeksu Pracy.

.....
(podpis osoby składającej oświadczenie)