

ZARZĄDZENIE NR 94/2024
WÓJTA GMINY GRUDZIĄDZ
z dnia 19 lipca 2024 r.

w sprawie organizacji pracy zdalnej okazjonalnej w Urzędzie Gminy Grudziądz

Na podstawie art. 33 ust. 3 i 5 ustawy z dnia 8 marca 1990 r. o samorządzie gminnym (Dz. U. z 2024 r., poz. 609 z późn. zm.) zarządzam, co następuje:

- §1.** 1. Pracownicy Urzędu Gminy Grudziądz mają prawo do korzystania z pracy zdalnej okazjonalnej w wymiarze 24 dni w roku kalendarzowym.
2. Przez pracę zdalną rozumie się pracę wykonywaną w miejscu wskazanym przez pracownika i każdorazowo uzgodnionym z pracodawcą, w tym pod adresem zamieszkania pracownika, w szczególności z wykorzystaniem środków bezpośredniego porozumiewania się na odległość.
 3. Wykonywanie pracy zdalnej okazjonalnej jest możliwe, jeśli organizacja pracy i rodzaj wykonywanej pracy na to pozwala.
 4. Okres wykonywania pracy zdalnej okazjonalnej jest ewidencjonowany. Niewykorzystane dni limitu pracy zdalnej okazjonalnej nie przechodzą na kolejny rok kalendarzowy.
 5. Skorzystanie z pracy zdalnej okazjonalnej wymaga złożenia wniosku przez pracownika w formie papierowej lub elektronicznej oraz uzyskania zgody Wójta Gminy Grudziądz. Wzór wniosku stanowi Załącznik nr 1 do niniejszego zarządzenia.
 6. Wójt może wyrazić zgodę na pracę zdalną okazjonalną pod warunkiem, że:
 - a) rodzaj/charakter pracy pozwala na jej okazjonalne wykonywanie w miejscu wskazanym przez pracownika;
 - b) pracownik posiada odpowiednie warunki techniczne i lokalowe do wykonywania pracy zdalnej okazjonalnej.
 7. Wniosek należy złożyć najpóźniej na 1 dzień przed rozpoczęciem pracy zdalnej. Zaakceptowany wniosek przekazywany jest do Referatu Organizacyjnego i Kadr w celu dołączenia do akt osobowych.
 8. Przed złożeniem wniosku pracownik zobowiązany jest do zapoznania się z:
 - a) procedurą ochrony danych osobowych w związku z wykonywaniem pracy zdalnej stanowiącą Załącznik nr 2 do niniejszego zarządzenia;
 - b) instrukcją określającą zasady bezpieczeństwa i higieny pracy podczas wykonywania pracy zdalnej stanowiącą Załącznik nr 3 do niniejszego zarządzenia.
 9. Miejsce wykonywania okazjonalnej pracy zdalnej powinno być ustalone z Wójtem. Pracownik każdorazowo ma obowiązek poinformowania o jego zmianie.
 10. Urząd Gminy Grudziądz nie ma obowiązku zapewnienia pracownikowi materiałów i narzędzi do wykonywania pracy zdalnej okazjonalnej, ich konserwacji czy pomocy technicznej, a także pokrycia kosztów ich zakupu, konserwacji i naprawy.
 11. Pracownik przed przystąpieniem do pracy na prywatnym komputerze, zobowiązany jest do złożenia "Oświadczenia pracownika wykonującego pracę zdalną na prywatnym komputerze", którego wzór stanowi Załącznik nr 4 do niniejszego zarządzenia.
- §2.** 1. Pracownik jest zobowiązany do wykonywania pracy zgodnie z treścią umowy o pracę / aktem powołania wiążącej go z Urzędem Gminy Grudziądz oraz zakresem obowiązków.

2. W celu zapewnienia komunikacji między pracownikami i procedowania spraw służbowych, w szczególności w celu przekazywania dokumentów wykorzystuje się środki komunikacji elektronicznej.
3. Do komunikacji elektronicznej używa się wyłącznie służbowego adresu mailowego w domenie @gruziadz.ug.gov.pl.
4. Na potrzeby wykonywania pracy zdalnej pracodawca określa procedurę ochrony danych osobowych oraz przeprowadza, w miarę potrzeby, instruktaż i szkolenie w tym zakresie. Pracownik wykonujący pracę zdalną okazjonalną potwierdza w postaci papierowej lub elektronicznej zapoznanie się z procedurami oraz jest zobowiązany do ich przestrzegania.

§3. 1. Pracownik wykonuje pracę zdalną okazjonalną w systemie czasu pracy i zgodnie z obowiązującym go rozkładem czasu pracy wynikającym z Regulaminu pracy.

2. Pracownika obowiązują przerwy w pracy wynikające z Regulaminu pracy.
3. Pracownik ma prawo do skorzystania z wyjścia prywatnego w związku z koniecznością załatwienia spraw prywatnych w ciągu dnia pracy. Wyjście prywatne jest udzielane na podstawie wniosku wysłanego mailem do bezpośredniego przełożonego i powinno być odpracowane w tym samym dniu roboczym.
4. Praca w godzinach nadliczbowych w czasie świadczenia pracy zdalnej może być wykonywana wyłącznie na zasadach określonych w Regulaminie pracy.

§4. Pracownik jest zobowiązany do:

- a) sprawdzenia (przed podjęciem pracy zdalnej okazjonalnej), że konta w aplikacjach oraz usługach online działają prawidłowo i umożliwiają zalogowanie;
- b) pozostawania w dyspozycji bezpośredniego przełożonego w ustalonych dniach i godzinach pracy oraz przyjmowania do realizacji bieżących zadań (np. w postaci plików tekstowych, skanów dokumentów);
- c) poświęcania czasu pracy wyłącznie na wykonywanie obowiązków pracowniczych, w tym poleceń bezpośredniego przełożonego, w szczególności na bieżąco sprawdzając korespondencję elektroniczną, odpowiadając na wiadomości, będąc w pełnej dostępności za pomocą służbowego telefonu lub adresu mailowego;
- d) bieżącego informowania o wykonywanych zadaniach oraz przedstawiania wyników swojej pracy na żądanie bezpośredniego przełożonego;
- e) potwierdzania obecności w pracy w okresie wykonywania pracy zdalnej okazjonalnej w sposób określony z bezpośrednim przełożonym;
- f) prowadzenia na polecenie Wójta ewidencji wykonanych czynności, uwzględniającej w szczególności opis tych czynności, a także datę oraz czas ich wykonania;
- g) przestrzegania zasad i przepisów dotyczących BHP i ochrony ppoż., w tym zorganizowania stanowiska pracy zdalnej z uwzględnieniem zasad ergonomii;
- h) powstrzymania się od wykonywania pracy w przypadku zaistnienia okoliczności powodującej zagrożenie życia i zdrowia a także niezwłocznego powiadomienia o tym bezpośredniego przełożonego;
- i) przestrzegania procedury ochrony danych osobowych w związku z wykonywanymi zadaniami;
- j) zabezpieczania dostępu do urządzeń, które wykorzystuje w celu pracy zdalnej oraz do posiadanych w związku z pracą zdalną dokumentów, danych i informacji przed

wszelkimi osobami postronnymi, w tym wspólnie z nim zamieszkującymi, jak również zabezpieczenia przed utraceniem, uszkodzeniem lub zniszczeniem urządzeń lub dokumentów;

- k) niezwłocznego zawiadomienia bezpośredniego przełożonego w przypadku kradzieży lub zgubienia urządzenia lub zaistnienia incydentu dotyczącego bezpieczeństwa danych osobowych.

§5. 1. Pracodawca ma prawo przeprowadzać kontrolę:

- a) wykonywania pracy zdalnej przez pracownika;
 - b) w zakresie bezpieczeństwa i higieny pracy zdalnej oraz przestrzegania wymogów w zakresie bezpieczeństwa i ochrony informacji, w tym procedur ochrony danych osobowych.
2. Kontrolę przeprowadza bezpośredni przełożony lub upoważniony pracownik ds. BHP i ochrony ppoż. na zasadach ustalonych z pracownikiem w miejscu wykonywania pracy zdalnej w godzinach pracy pracownika.
 3. Wykonywanie czynności kontrolnych nie może naruszać prywatności pracownika wykonującego pracę zdalną i innych osób ani utrudniać korzystania z pomieszczeń domowych w sposób zgodny z ich przeznaczeniem.
 4. Kontrola może mieć charakter kontroli online, odbywającej się przez telekonferencję za pośrednictwem telefonu komórkowego.
 5. Jeżeli przeprowadzający kontrolę stwierdzi uchybienia w przestrzeganiu przepisów i zasad w zakresie bezpieczeństwa i higieny pracy lub w przestrzeganiu wymogów w zakresie bezpieczeństwa i ochrony informacji, zobowiązuje pracownika do usunięcia stwierdzonych uchybień we wskazanym terminie.
 6. Przeprowadzający kontrolę powinien sporządzić szczegółowy protokół, w którym zostaną opisane wszystkie nieprawidłowości, jakie stwierdzono w trakcie dokonywanych czynności kontrolnych.
 7. Z przeprowadzonej kontroli nie sporządza się protokołu, jeśli w trakcie podjętych działań nie stwierdzono żadnych nieprawidłowości.

§6. Zgłoszenie wypadku przy pracy zdalnej następuje na zasadach określonych w Regulaminie pracy Urzędu Gminy Grudziądz.

§7. 1. Wójt cofa zgodę na wykonywanie pracy zdalnej okazjonalnej w przypadku:

- a) gdy zostanie poinformowany przez pracownika o zmianie warunków lokalowych i technicznych uniemożliwiających wykonywanie pracy zdalnej;
 - b) braku usunięcia przez pracownika stwierdzonych uchybień, po przeprowadzonej kontroli.
2. W przypadku cofnięcia zgody na wykonywanie pracy zdalnej okazjonalnej, pracownik rozpoczyna pracę niezwłocznie w dotychczasowym miejscu pracy określonym w umowie o pracę / akcie powołania.

Wójt

/-/Andrzej Rodziewicz

.....
(imię i nazwisko pracownika)

Grudziądz, dnia r.

.....
(stanowisko pracy)

.....
(jednostka organizacyjna)

WNIOSEK

o wykonywanie okazjonalnej pracy zdalnej

Na podstawie art. 67³³ Kodeksu pracy składam wniosek o wykonywanie okazjonalnej pracy zdalnej w dniu* lub w okresie* od dnia do dnia

Praca zdalna będzie wykonywana pod adresem:

.....
Oświadczam, że:

1. Na stanowisku pracy zdalnej, w miejscu jej wykonywania są zapewnione bezpieczne i higieniczne warunki tej pracy.
2. Zapoznałem/am się z przygotowaną przez pracodawcę:
 - a) procedurą ochrony danych osobowych w związku z wykonywaniem pracy zdalnej,
 - b) instrukcją określającą zasady bezpieczeństwa i higieny pracy podczas wykonywania pracy zdalnej.
3. Zobowiązuję się do przestrzegania informacji, procedur oraz wskazówek wynikających z dokumentów wskazanych w pkt 2.
4. Zasady kontroli wykonywania pracy zdalnej, kontrola w zakresie bezpieczeństwa i higieny pracy są mi znane i potwierdzam wolę ich stosowania w czasie wykonywania pracy w zdalnej.
5. Pracę zdalną będę wykonywać na komputerze zapewnionym przez Pracodawcę / prywatnym**.

.....
(podpis pracownika)

Potwierdzam, że organizacja pracy i rodzaj pracy umożliwia wykonywanie pracy zdalnej i wyrażam zgodę.

.....
(pieczęć i podpis Wójta)

* niepotrzebne skreślić

** w przypadku wykonywania pracy zdalnej na komputerze prywatnym, należy dołączyć oświadczenie, którego wzór stanowi Załącznik nr 4 do zarządzenia Wójta Gminy Grudziądz nr 94/2024 z dnia 19 lipca 2024 r.

Procedura ochrony danych osobowych w związku z wykonywaniem pracy zdalnej

§1. Postanowienia ogólne dotyczące pracy zdalnej

1. Praca zdalna to taka praca, która może być wykonywana całkowicie lub częściowo w miejscu wskazanym przez Użytkownika i każdorazowo uzgodnionym z pracodawcą, w tym pod adresem zamieszkania Użytkownika, w szczególności z wykorzystaniem środków bezpośredniego porozumiewania się na odległość.
2. Użytkownicy podczas pracy zdalnej mogą przetwarzać dane osobowe tylko w celach związanych z wykonywaniem swoich obowiązków służbowych oraz są zobowiązani zapewnić bezpieczeństwo tych danych, przestrzegając zasad wynikających z niniejszej Polityki oraz innych procedur przyjętych w tym zakresie w Jednostce.
3. Użytkownicy w trakcie pracy zdalnej zobowiązani są dbać o należyte bezpieczeństwo danych osobowych w szczególności o ich dostępność, poufność oraz integralność.
4. Użytkownicy zobowiązani są do zgłaszania bezpośrednio przełożonemu każdego potencjalnego incydentu lub zdarzenia, skutkującego wystąpieniem naruszenia ochrony danych osobowych zgodnie z procedurą stanowiącą załącznik nr 14 do Polityki ochrony danych osobowych, tak aby Administrator mógł się wywiązać z obowiązków nałożonych na niego na mocy art. 33 RODO.
5. Użytkownik, który składa wniosek na wykonywanie pracy zdalnej jest informowany o przetwarzaniu jego danych osobowych do tego celu.

§2. Praca na dokumentacji papierowej i elektronicznej w ramach wykonywania pracy zdalnej

1. Użytkownicy nie powinni wnosić oryginalnej dokumentacji stanowiącej własność Jednostki w postaci papierowej poza określony przez Administratora obszar przetwarzania danych bez pisemnej zgody bezpośredniego przełożonego lub innego upoważnionego przedstawiciela Administratora.
2. Jeżeli Administrator dopuszcza przy pracy zdalnej możliwość korzystania przez Użytkowników z dokumentacji papierowej, w tym również kopii dokumentów, wówczas Administrator zobowiązany jest:
 - 1) ewidencjonować wydane Użytkownikom dokumenty na potrzeby pracy zdalnej;
 - 2) poinformować Użytkowników o obowiązku ograniczonego przechowywania wydanych im dokumentów jedynie przez okres niezbędny do wykonania określonego zadania podczas pracy zdalnej (ograniczenie przechowywania);
 - 3) zobowiązać Użytkowników do wykorzystywania podczas pracy zdalnej pozyskanych dokumentów zawierających dane osobowe wyłącznie w takim celu, w jakim byłyby one wykorzystywane w siedzibie Administratora;
 - 4) ograniczyć liczbę dokumentów wnoszonych poza obszar przetwarzania danych do tego, co niezbędne w stosunku do celu, w jakim te dane osobowe są przetwarzane przez Użytkownika w ramach wykonywania pracy zdalnej;

- 5) zobowiązać Użytkownika do odpowiedniego zabezpieczenia danych osobowych podczas wykonywania pracy zdalnej, w szczególności przed dostępem osób nieuprawnionych.
3. Użytkownik zobowiązany jest do zwrotu kopii dokumentów.
4. Praca zdalna na dokumentach papierowych przez Użytkownika będzie nieuzasadniona jeżeli Administrator:
 - 1) wdrożył elektroniczny obieg dokumentów lub posiada możliwość szybkiego, sprawnego i bezpiecznego wdrożenia elektronicznego obiegu dokumentacji w zakresie związanym z obowiązkami Użytkownika;
 - 2) Użytkownik posiada bezpieczny szyfrowany dostęp do niezbędnych do pracy dokumentów, w tym danych osobowych, przy pomocy środków komunikacji elektronicznej;
 - 3) udostępnił Użytkownikowi odpowiednio zabezpieczone (m.in. zaszyfrowane) elektroniczne kopie niezbędnych dokumentów.

§3. Zasady bezpieczeństwa stosowane w ramach wykonywania pracy zdalnej

1. W ramach pracy zdalnej Użytkownicy mają obowiązek przestrzegać następujących zasad bezpiecznej pracy zdalnej:
 - 1) zakazuje się wnosić oryginalnej dokumentacji stanowiącej własność Jednostki w postaci papierowej poza określony przez Administratora obszar przetwarzania danych bez pisemnej zgody bezpośredniego przełożonego lub innego upoważnionego przedstawiciela Administratora;
 - 2) zapewnienie sobie w miejscu pracy przestrzeni, odpowiedniej do tego, aby osoby postronne nie miały dostępu do informacji służbowych;
 - 3) prowadzenie rozmów i wideokonferencji służbowych powinno odbywać się w pomieszczeniach wewnętrznych bez dostępu osób nieupoważnionych przez Administratora do przekazywanych informacji (np. poprzez prowadzenie rozmów w odrębnym pokoju, a w przypadku wideokonferencji również w słuchawkach);
 - 4) zakazane jest prowadzenie służbowych rozmów telefonicznych, w tym wideokonferencji, w miejscach narażonych na brak poufności informacji w szczególności np. na balkonach, tarasach czy innych otwartych przestrzeniach;
 - 5) zakazane jest udostępnianie służbowych urządzeń osobom nieupoważnionym przez Administratora, w tym członkom rodziny Użytkownika;
 - 6) zakazane jest niszczenie dokumentacji papierowej w miejscu pracy zdalnej – tego rodzaju czynności powinny odbywać się wyłącznie w siedzibie Administratora;
 - 7) dokumentacja w formie papierowej oraz nośniki elektroniczne powinny być bezpiecznie przechowywane (np. szafa lub szuflada zamykana na klucz lub inne miejsca niedostępne dla pozostałych domowników Użytkownika);
 - 8) zakazane jest udostępnianie osobom nieupoważnionym przez Administratora treści wyświetlanych na ekranie komputera, który jest wykorzystywany do pracy zdalnej – należy przestrzegać zasady „czystego ekranu”, a także zadbać o odpowiednie ustawienie ekranu i/lub zastosowanie filtra prywatyzującego przekazanego przez Administratora;
 - 9) przestrzeganie polityki „czystego biurka”;

- 10) zakazane jest pozostawianie komputera używanego do pracy zdalnej bez nadzoru, a w przypadku krótkotrwałego opuszczenia stanowiska pracy zablokowanie go i zabezpieczenie dokumentów, konta systemowe powinny być blokowane przed każdorazowym odejściem Użytkownika od stanowiska pracy;
- 11) wygaszacz ekranu powinien być uruchamiany automatycznie po upływie oznaczonego czasu w razie braku aktywności Użytkownika;
- 12) komputer służący do pracy zdalnej powinien być zabezpieczony przed dostępem osób nieupoważnionych przez Administratora z wykorzystaniem indywidualnego identyfikatora oraz hasła Użytkownika (podobne zasady obowiązują w zakresie telefonu wykorzystywanego do celów pracy zdalnej poprzez stosowanie PIN-u lub innej formy uwierzytelniania, używanie do logowania się na komputerze haseł zgodnych z polityką haseł przyjętą w Jednostce);
- 13) zakazane jest udostępnianie przez Użytkownika haseł osobom postronnym;
- 14) nośniki elektroniczne i urządzenia mobilne (w tym pendrive'y, karty pamięci, laptopy, telefony i tablety) powinny być szyfrowane;
- 15) używanie tylko rekomendowanych przez administratora przeglądarek internetowych;
- 16) nie zapamiętywanie haseł w przeglądarkach internetowych;
- 17) nie wykorzystywanie komputera do prywatnych celów (np. zakupy, gry, itp.);
- 18) nie instalowanie żadnego oprogramowania bez uprzedniej akceptacji przez Obsługę informatyczną;
- 19) nie logowanie się komputerem do publicznych sieci Wi-Fi;
- 20) łączenie się z zasobami Jednostki tylko za pomocą skonfigurowanego przez Administratora bezpiecznego łącza VPN;
- 21) korzystanie do celów służbowych tylko ze służbowej poczty e-mail;
- 22) przed wysłaniem wiadomości upewnienie się, że jest ona wysyłana do właściwego adresata, szczególnie gdy wysyłane są dane osobowe lub inne istotne informacje;
- 23) nie otwieranie wiadomości pochodzących od nieznanego nadawcy, a szczególnie załączników niewiadomego pochodzenia oraz nie klikanie w żadne linki lub odnośniki;
- 24) w przypadku przesyłania plików lub dokumentów za pomocą poczty e-mail lub komunikatora internetowego – każdorazowo zabezpieczanie je hasłem (hasło należy przekazać innym kanałem kontaktowym np. wiadomością SMS);
- 25) dokumentacja i inne źródła danych osobowych nie mogą być wykorzystywane przez Użytkownika w publicznych chmurach obliczeniowych, komunikatorach lub innych usługach dostępnych w sieci publicznej, które nie zostały uprzednio autoryzowane przez Administratora;
- 26) zakazane jest utrwalanie danych na lokalnym dysku komputera – możliwość wykorzystania wyłącznie wskazanych przez Administratora zasobów sieciowych, z których wykonywane są regularnie kopie zapasowe;
- 27) stosowanie rozwiązań umożliwiających zdalne zarządzanie urządzeniami mobilnymi, w tym ich zdalne zlokalizowanie lub przywrócenie do stanu fabrycznego;

- 28) sprzęt informatyczny powinien zostać wyposażony w uruchomione oprogramowanie antywirusowe i zaporę sieciową;
- 29) użytkowana wersja systemu operacyjnego winna być wspierana przez producenta;
- 30) obowiązek aktualizowania systemu operacyjnego, z których korzysta Użytkownik, w tym systemu antywirusowego;
- 31) zakazane jest samodzielne pobieranie i instalacja oprogramowania bez wyraźnej zgody Administratora;
- 32) co do zasady zakazane jest korzystanie z uprawnień administratora na komputerach służbowych wykorzystywanych do pracy zdalnej (chyba, że nie istnieje odmienna możliwość korzystania z urządzenia lub systemu teleinformatycznego);
- 33) zakazane jest naprawianie sprzętu informatycznego, na którym znajdują się dane osobowe Administratora z wykorzystaniem wsparcia podmiotów zewnętrznych bez uzyskania uprzedniej pisemnej zgody Administratora;
- 34) zakazane jest drukowanie dokumentów służbowych w punktach ksero lub z pomocą innych podmiotów/osób trzecich;
- 35) zakaz drukowania oraz skanowania dokumentów w miejscu pracy zdalnej chyba, że ADO oprócz komputera udostępni pracownikowi także urządzenia peryferyjne np. drukarkę, skaner itp.; obowiązek zabezpieczenie wydruków technicznych lub błędnie wykonanych – do momentu powrotu do pracy, a następnie zniszczenie ich w niszczarce;
- 36) w przypadku wykorzystywania do kontaktów komunikatora internetowego – nie używanie w tym samym czasie innych narzędzi do komunikacji – z zastrzeżeniem pkt. 25;
- 37) użytkowanie sprzętu informatycznego powinno być zgodne z zasadami ostrożności z uwagi na konieczność uwzględnienia zagrożeń sieciowych typu phishing, na które sieć domowa może być bardziej podatna niż sieć Administratora;
- 38) w przypadku utraty sprzętu – natychmiastowe skontaktowanie się z osobą wyznaczoną do kontaktu i zadbanie – w miarę możliwości – o zdalne usunięcie danych z urządzenia.

§4. Postanowienia końcowe

1. Obsługa informatyczna Jednostki lub inna osoba upoważniona przez Administratora prowadzi wykaz sprzętu (np. laptopy, smartfony) wydanego Użytkownikowi na potrzeby pracy zdalnej.
2. Obsługa informatyczna Jednostki zapewnia, aby sprzęt wydawany Użytkownikowi został wcześniej odpowiednio skonfigurowany, zabezpieczony przed ujawnieniem lub utratą danych, zgodnie z Instrukcją zarządzania systemami informatycznymi oraz innymi dokumentami dotyczącymi bezpieczeństwa sprzętu przyjętymi w Jednostce.
3. Obsługa informatyczna Jednostki przygotowuje dla Użytkowników pracujących zdalnie instrukcję dotyczącą instalacji, inwentaryzacji, konserwacji, aktualizacji oprogramowania i serwisu powierzonych Użytkownikowi narzędzi pracy, w tym urządzeń technicznych.

4. Użytkownik jest zobowiązany stosować się do ustalonych przez Administratora zasad dotyczących instalacji, inwentaryzacji, konserwacji, aktualizacji oprogramowania i serwisu powierzonych mu narzędzi pracy, w tym urządzeń technicznych.

Instrukcja określająca zasady bezpieczeństwa i higieny pracy podczas wykonywania pracy zdalnej






§1. Organizacja stanowiska pracy zdalnej z uwzględnieniem ergonomii








1. Przed rozpoczęciem pracy w trybie zdalnym, pracownik ma obowiązek sprawdzić czy jego stanowisko pracy odpowiada warunkom bezpieczeństwa, w tym przede wszystkim czy jest zgodne z wymaganiami ergonomii.
2. Usytuowanie stanowiska pracy:
 - 1) komputerowe stanowisko pracy powinno być tak usytuowane, aby pracownik miał do niego swobodny dostęp. Wyposażenie pomieszczenia pracy nie powinno powodować trudności w poruszaniu się skutkującymi koniecznością przeciskania się czy przeskakiwania nad elementami wyposażenia. W przeciwnym razie nietrudno o wypadek przy pracy;
 - 2) pomocne jest oddzielenie strefy pracy od strefy relaksu – nie należy stawiać komputera w sypialni, powinna zostać wytyczona w mieszkaniu choćby niewielka przestrzeń na własne biuro.
3. Informacje ogólne:
 - 1) przed przystąpieniem po raz pierwszy do obsługi urządzenia należy uważnie zapoznać się z instrukcją obsługi dostarczaną przez producenta;
 - 2) do pracy z komputerem może być dopuszczony pracownik, który posiada orzeczenie lekarskie o braku przeciwwskazań zdrowotnych;
 - 3) średnie natężenie oświetlenia światłem sztucznym w pomieszczeniu z monitorami ekranowymi oraz na stanowisku pracy wyposażonym w komputer powinno wynosić 500 lx;
 - 4) dopuszczalna wartość hałasu w pomieszczeniach do zwykłych prac biurowych powinna wynosić 75 dB.;
 - 5) przy pracy z laptopem stanowisko musi być wyposażone w monitor komputerowy lub w podstawkę na laptopa oraz mysz i osobną klawiaturę.
4. Na stanowisku pracy zabrania się:
 - 1) samodzielnego naprawiania urządzeń i wyposażenia stanowiskowego zasilanych energią elektryczną;
 - 2) czyszczenia na mokro obudowy urządzeń będących pod napięciem oraz używania do czyszczenia rozpuszczalników organicznych;
 - 3) noszenia oraz przechowywania przy komputerze magnesów i biżuterii magnetycznej;
 - 4) instalowania i wykorzystania oprogramowania bez licencji.
5. Czynności do wykonania przed rozpoczęciem pracy:
 - 1) sprawdzić kompletność technicznego wyposażenia stanowiska pracy oraz stan kabli zasilających komputer i urządzenia współpracujące;

- 2) sprawdzić, czy elementy wyposażenia komputera zapewniają bezpieczeństwo pracy, w tym ochronę przed porażeniem prądem elektrycznym;
- 3) dopasować fotel, biurko i klawiaturę do antropometrycznych właściwości własnego ciała zapewniając wygodną pozycję ciała i swobodę ruchów;
- 4) zapewnić:
 - a) wystarczającą powierzchnię do łatwego posługiwania się elementami wyposażenia stanowiska pracy oraz takie ich ustawienie, by znajdowały się w zasięgu rąk, bez konieczności przyjmowania wymuszonych pozycji;
 - b) ustawienie klawiatury z zachowaniem odległości nie mniejszej niż 100 mm między klawiaturą a przednią krawędzią stołu (biurka);
 - c) odległość oczu od ekranu monitora w granicach 40–75 cm;
- 5) oczyścić ekran monitora z kurzu, wyregulować jaskrawość i kontrast na ekranie w zależności od warunków oświetlenia stanowiska pracy. Zapewnić, by obraz na ekranie był stabilny;
- 6) przygotować i uruchomić programy zgodnie z instrukcjami ich użytkowania.

§2. Zasady bezpiecznego i higienicznego wykonywania pracy zdalnej

1. Pracując zdalnie, pracownik może być narażony na zagrożenia zawodowe występujące w procesie pracy. Pracownik ma obowiązek znać te zagrożenia i stosować działania ograniczające prawdopodobieństwo ich wystąpienia.
2. Zagrożenia wraz z działaniami zapobiegawczymi zostały zestawione w tabeli poniżej:

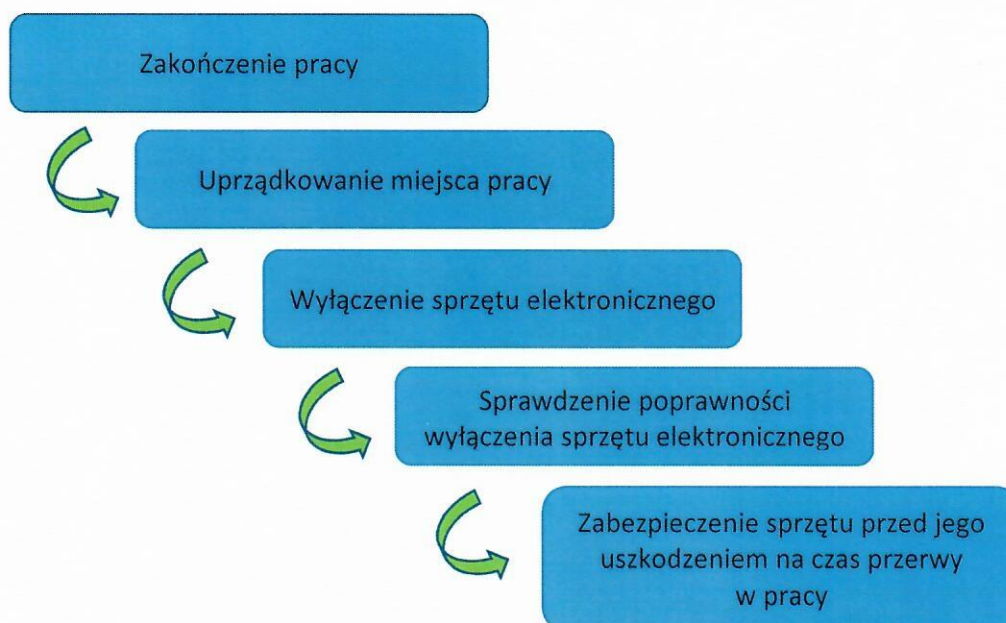
L.p.	Zagrożenie	Opis	Działania zapobiegawcze
1		Gorące powierzchnie	<ul style="list-style-type: none"> Przygotowanie posiłków poza stanowiskiem pracy.
2		Energia elektryczna	<ul style="list-style-type: none"> Używanie podczas pracy tylko sprawnego wyposażenia. Przestrzeganie zakazu wykonywania samodzielnych napraw wyposażenia stanowiska pracy.
3		Zalegające przedmioty	<ul style="list-style-type: none"> Utrzymywanie porządku.
4		Elementy ruchome urządzeń	<ul style="list-style-type: none"> Korzystając np. z niszczarki nie wolno pracować w zbyt luźnej odzieży.
5		Upadek na niższy poziom	<ul style="list-style-type: none"> Korzystanie ze stopni/podestów przy ściąganiu przedmiotów z poziomu wyżej.

6		Ostre krawędzie	<ul style="list-style-type: none"> • Używanie podczas pracy tylko sprawnego wyposażenia.
7		Spadające przedmioty np. z półki	<ul style="list-style-type: none"> • Utrzymanie porządku na stanowisku pracy.
8		Upadek na niższy poziom	<ul style="list-style-type: none"> • Trzymanie się poręczy podczas poruszania się po schodach.
9		Hałas	<ul style="list-style-type: none"> • Używanie słuchawek zestawu komputerowego. • Odizolowanie stanowiska pracy w przestrzeni domowej.
10		Praca siedząca	<ul style="list-style-type: none"> • Ergonomiczne stanowisko pracy. • Przerwy w pracy.
11		Pożar	<ul style="list-style-type: none"> • Zakaz używania otwartego ognia na stanowisku pracy.
12		Stres psychospołeczny	<ul style="list-style-type: none"> • Poprawa znajomości oprogramowania oraz sprzętu komputerowego.

- Po każdej godzinie nieprzerwanej pracy związanej z obsługą komputera stosować co najmniej 5-minutowe przerwy (wliczane do czasu pracy).
- W przypadku awarii lub uszkodzenia w części zasilającej lub elektronicznej komputera natychmiast wyłączyć zasilanie i niezwłocznie poinformować przełożonego (administrатора sieci).

§3. Czynności do wykonania po zakończeniu wykonywania pracy zdalnej

1. Po zakończeniu pracy pracownik ma obowiązek postępować zgodnie ze schematem poniżej:



§4. Zasady postępowania w sytuacjach awaryjnych

1. Przez sytuację awaryjną należy rozumieć każdą sytuację stanowiącą zagrożenie dla życia i zdrowia pracownika oraz jego najbliższego otoczenia.
2. Poniżej opisano sposoby postępowania w przypadku wypadku, pożaru oraz ulatniania się gazu:

L.p.	Sytuacja awaryjna	Sposób postępowania
1	Wypadek przy pracy	<ol style="list-style-type: none">1. W zależności od rodzaju urazu, pracownik może udzielić sobie samodzielnie pierwszej pomocy lub wezwać pogotowie ratunkowe, jeżeli jest to niezbędne, numer 112.2. Poinformowanie przełożonego najszybciej jak to jest możliwe.
2	Pożar	<ol style="list-style-type: none">1. Odcięcie źródeł energii.2. Podjęcie próby ugaszenia pożaru niewielkich rozmiarów.3. Przy dużych pożarach natychmiast należy się ewakuować poza strefę zagrożenia i zadzwonić na numer alarmowy 112. Dzwoniąc należy podać:<ul style="list-style-type: none">– swoje imię i nazwisko, numer telefonu, z którego przekazywana jest informacja o zdarzeniu;– adres i nazwę obiektu, w którym powstał pożar;– co się pali, na którym piętrze;– czy występuje zagrożenie dla życia i zdrowia ludzkiego.4. Podczas ewakuacji nie wolno używać windy.5. Dalsze postępowanie zgodnie z instrukcjami straży pożarnej.

3	Ulatnianie się gazu	<ol style="list-style-type: none">1. Zawiadomić jak najszybciej pogotowie gazowe (992) i administrację.2. Nie włączać światła ani żadnych urządzeń elektrycznych.3. Nie zapalać zapalek czy zapalniczek.4. Zamknąć zawór gazu w mieszkaniu.5. Wyjść na zewnątrz budynku.
---	----------------------------	--

§5. Kontrole pracy zdalnej w zakresie warunków pracy, BHP na stanowisku

Pracodawca ma prawo przeprowadzać kontrolę wykonywania pracy zdalnej przez pracownika, w zakresie bezpieczeństwa i higieny pracy. Kontrola pracy zdalnej organizowana jest w porozumieniu z pracownikiem, na zasadach wewnętrznie ustalonych porozumieniem w sprawie pracy zdalnej.

.....
(imię i nazwisko pracownika)

Grudziądz, dnia r.

.....
(stanowisko pracy)

.....
(jednostka organizacyjna)

**Oświadczenie pracownika
wykonującego pracę zdalną na prywatnym komputerze**

Oświadczam, że:

1. Posiadany przeze mnie komputer przenośny / stacjonarny*

.....
będzie użytkowany przeze mnie z zachowaniem obowiązujących przepisów prawa. Nie będę przechowywał/a na nim danych osobowych pracowników Urzędu Gminy Grudziądz ani żadnych innych treści poufnych lub strategicznych dotyczących działalności Urzędu.

2. Komputer posiada legalne i stale aktualizowane oprogramowanie antywirusowe, pozostałe zainstalowane i użytkowane na nim oprogramowanie jest również legalne (w przypadku kontroli posiadam dowody legalności/zakupu oprogramowania).
3. Będę dokładać starań, by komputer ten nie stał się zagrożeniem dla innych użytkowników (np. poprzez rozsyłanie wirusów, umożliwienie przejęcia nad nim zdalnej kontroli osobom postronnym spowodowane obecnością oprogramowania złośliwego lub niewłaściwego zabezpieczenia systemu).
4. Przyjmuję do wiadomości, że Urząd nie jest zobligowany do zapewnienia na prywatnych komputerach pracowników oprogramowania potrzebnego do pracy.
5. W przypadku naruszenia któregokolwiek z powyższych punktów i przyjętych w Urzędzie zasad oraz przepisów obowiązującego prawa jestem świadomy/a wynikających z tego konsekwencji prawnych.

.....
(podpis pracownika)