ZARZĄDZENIE NR 75/2020
WÓJTA GMINY GNIEZNO

z dnia 27 października 2020 r.

wprowadzające rozwiązania organizacyjno-techniczne dotyczące wykonywania pracy zdalnej w Urzędzie Gminy Gniezno na czas zagrożenia epidemicznego

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) , art. 33 ust. 3 i 5 ustawy z dnia 8 marca 1990 r. o samorządzie gminnym (t.j. Dz. U. z 2019 r. poz. 506 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 na terenie Polski i możliwym potencjalnym zagrożeniem dla zdrowia pracowników Urzędu Gminy Gniezno wirusem SARS-CoV-2, wprowadzam możliwość pracy zdalnej, z wykorzystaniem służbowego lub prywatnego sprzętu komputerowego pracowników Urzędu Gminy Gniezno.

2. Zasady pracy Urzędu w czasie zagrożenia epidemicznego 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 kierownik referatu, w uzgodnieniu z Sekretarzem Urzędu.

4. W stosunku do osób zatrudnionych na stanowiskach kierowniczych oraz na samodzielnych stanowiskach, decyzję o rozpoczęciu i zakończeniu pracy zdalnej podejmuje Wójt Gminy Gniezno.

§ 2. 1. Przyjęte rozwiązania organizacyjno-techniczne dotyczące pracy zdalnej obowiązują w czasie zagrożenia epidemicznego lub do odwołania w drodze zarządzenia.

2. W przypadku wystąpienia uzasadnionych okoliczności wymagających wydłużenia terminu wskazanego w ust. 1, informacja o tym fakcie zostanie zakomunikowana pracownikom Urzędu korzystającym z pracy zdalnej, w tym drogą elektroniczną, pocztą e-mailową, bez konieczności zmiany niniejszego zarządzenia.

§ 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 Gminy Gniezno do zapoznania się z treścią i stosowania niniejszego zarządzenia.

§ 4. Wykonanie zarządzenia powierza się Sekretarzowi Urzędu Gminy Gniezno.

§ 5. Traci moc Zarządzenie Nr 19/2020 Wójta Gminy Gniezno z dnia 1 kwietnia 2020 r. w sprawie zmian w organizacji i systemu pracy pracowników Urzędu Gminy Gniezno.

§ 6. Zarządzenie wchodzi w życie z dniem podpisania.

Wójt Gminy Gniezno

Maria Suplicka

Załącznik do zarządzenia Nr 75/2020

Wójta Gminy Gniezno

z dnia 27 października 2020 r.

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 na terenie Polski i możliwym potencjalnym zagrożeniem dla zdrowia pracowników Urzędu Gminy Gniezno 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: smartfon, tablet, IPad)(zwanej dalej „pracą zdalną").

3. 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 wymagające dostępu do zasobów sprzętowych i informacyjnych organizacji. Pod określeniem "pracodawca" należy rozumieć zarówno pracodawcę, jak i zlecającego usługi.

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, w tym zakres i harmonogram wykonywanej pracy określa pracodawca, jednakże pracownik może także zaproponować własny harmonogram i zakres pracy, który będzie mógł realizować po uzyskaniu zgody pracodawcy.

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 Administratora Systemów Informatycznych (ASI)/Informatyka wyznaczonego u pracodawcy, 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, a w przypadkach uzasadnionych zakresem obowiązków lub stanowiskiem służbowym również do programów dedykowanych (np. w zakresie rozliczeń księgowych).

9. Złamanie zasad określonych w Regulaminie lub niedostosowanie się do postanowień niniejszego Regulaminu może stanowić 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 zawodowym profesjonalizmem i skutkować rozwiązaniem umowy, a także przewidzianymi w umowie karami umownymi.

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, smartfona, tableta Ipada, 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 tableta Ipada, należy upewnić się, że urządzenie zostało zablokowane.

IV. Bezpieczeństwo pracy zdalnej

1. Pracownik wykonuję 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, w szczególności:

a) Korzystanie z Internetu powinno wymagać uwierzytelnienia, np. poprzez hasło,

b) Hasło dostępu powinno składać się z co najmniej 8 znaków, w tym z dużych i małych liter oraz cyfr i znaków specjalnych,

c) Jeśli to możliwe, należy zmienić login do panelu administracyjnego routera na własny,

d) Dostęp do panelu administracyjnego routera jest możliwy wyłącznie z urządzeń znajdujących się w sieci domowej,

e) Został zmieniony domyślny adres routera (najczęściej 192.168.1.1.) na inny,

f) Porad i wsparcia w zakresie konfiguracji sieci domowej, w tym jej zabezpieczenia na potrzeby pracy zdalnej udziela Administrator Systemu Informatycznego (ASI)/Informatyk wyznaczony u pracodawcy.

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, z zastosowaniem stosownego oprogramowania (np. Eraser),

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) niewykonywania jednocześnie działań służbowych oraz prywatnych na tym samym komputerze; nie wykonywania pracy służbowej z własną aktywnością osobistą na przykład na portalach społecznościowych np. Facebooku,

n) unikania przeglądania stron potencjalnie niebezpiecznych,

o) nieużywania prywatnych skrzynek pocztowych czy grup na portalach społecznościowych do komunikacji firmowej,

p) w przypadku wykonywania pracy zdalnej w sposób inny niż z wykorzystaniem pulpitu zdalnego (np. w drodze dostępu do aplikacji służbowych za pomocą strony internetowej – poczty służbowej) – niezapisywania jakichkolwiek danych pracodawcy poza aplikacjami, w których taki zapis jest elementem ich funkcjonowania (np. zapisanie się wysłanego e-maila w katalogu wysłane). W szczególności zapisywania jakichkolwiek danych pracodawcy na dyskach prywatnego komputera, prywatnych nośnikach zewnętrznych lub na prywatnym koncie w usłudze chmurowej (np. Google Drive, iCloud, Microsoft Onedrive, Dropbox),

q) 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 do Administratora Systemu Informatycznego (ASI)/Informatyka wyznaczonego u pracodawcy.

2. W przypadku zgubienia lub kradzieży sprzętu, dokumentów lub innych nośników informacji, należy niezwłocznie, w dniu zdarzenia zgłosić zdarzenie do pracodawcy, Administratora Systemu Informatycznego (ASI)/Informatyka wyznaczonego przez pracodawcę, a także inspektora ochrony danych.

VIII. Działania niedozwolone

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 Administratorowi Systemu Informatycznego (ASI)/Informatykowi wyznaczonemu przez pracodawcę, przeglądu urządzenia,

6. Niszczenie dokumentów w domu,

7. Udostępnianie służbowego sprzętu lub sprzętu wykorzystywanego do realizowania zadań służbowych innym osobom,

8. Dzielenie się informacjami poufnymi z innymi osobami, w szczególności domownikami,

9. Samodzielne zniszczenie dokumentów w domu,

10. Logowanie się na konto innego użytkownika,

11. Zabranie dokumentów bez pisemnej lub elektronicznej zgody pracodawcy,

12. Zabranie oryginałów dokumentów,

13. Niezwrócenie dokumentów,

14. Niepotwierdzenie z pracodawcą zakresu zwróconych danych.