ZARZĄDZENIE NR 1/2020
KIEROWNIKA GMINNEGO OŚRODKA POMOCY SPOŁECZNEJ

z dnia 27 marca 2020 r.

w sprawie organizacji pracy w Gminnym Ośrodku Pomocy Społecznej w Warlubiu w okresie obowiązywania stanu epidemii na terenie Rzeczypospolitej Polskiej

Na podstawie § 5 pkt. 7 Statutu Gminnego Ośrodka Pomocy Społecznej w Warlubiu uchwalonego uchwałą Nr XVIII/92/2016 Rady Gminy Warlubie z dnia 17 marca 2016 r. w związku z art. 3 ustawy o szczególnych rozwiązaniach związanych z zapobieganiem, przeciwdziałaniem i zwalczaniem Covid-19, innych chorób zakaźnych oraz wywołanych nimi sytuacji kryzysowych, z dnia 2 marca 2020 r. (Dz.U. z 2020 r. poz. 374) oraz § 10 ust. 1 i 2 rozporządzenia Ministra Zdrowia z dnia 20 marca 2020 r. w sprawie ogłoszenia na obszarze Rzeczypospolitej Polskiej stanu epidemii zarządzam, co następuje:

§ 1. Ustala się sposób organizacji wewnętrznej pracy Gminnego Ośrodka Pomocy Społecznej w Warlubiu na czas występowania zagrożenia zarażeniem COVID-19, w celu przeciwdziałania jego rozprzestrzeniania.

§ 2. 1. Wprowadza się ograniczenie w przyjmowaniu interesantów w GOPS.

2. Podstawowym sposobem kontaktu z GOPS jest telefon, e-mail oraz platforma Epuap.

3. Zakazuje się wstępu osobom postronnym do budynku GOPS z zastrzeżeniem poniższych postanowień.

4. Wstęp do GOPS w celu załatwienia sprawy jest możliwy wyłącznie za zgodą właściwego pracownika GOPS. W tym celu należy skontaktować się z danym pracownikiem GOPS, opisać przedmiot sprawy i uzgodnić datę wizyty.

5. Każdy interesant przed wejściem do GOPS, jest zobowiązany podać swoje dane osobowe oraz wypełnić ankietę związaną z badaniem możliwości kontaktu danej osoby z wirusem COVID-19.

6. Przed wejściem do budynku GOPS interesant jest zobowiązany do poddania się odległościowemu badaniu pomiaru temperatury ciała.

7. Pomiaru dokonuje pracownik GOPS, odpowiednim przyrządem.

8. W przypadku, gdy wynik pomiaru przekracza 37 stopni Celsjusza, pracownik może odmówić dostępu do budynku.

9. Odmowa wykonania czynności wskazanych w ust. 5 i 6, uniemożliwia wstęp osoby trzeciej do budynku.

10. W pierwszym korytarzu w budynku GOPS wystawiona zostaje skrzynia podawcza, do której interesanci mogą składać pisma kierowane do GOPS. Skrzynia podawcza jest opróżniana następnego dnia o godzinie 8^{00}.

§ 3. 1. Wprowadza się pracę zdalną dla pracowników GOPS.

2. Pracownicy wyznaczeni przez Kierownika GOPS świadczą pracę zdalnie, w miejscu zamieszkania lub pobytu, przez okres wskazany przez Kierownika GOPS.

3. Dobowy czas pracy może być podzielony pomiędzy pracą zdalną i pracą w GOPS.

4. W trakcie świadczenia pracy zdalnej, pracownik pozostaje do dyspozycji Kierownika GOPS, który może go wezwać do stawiennictwa w budynku GOPS.

5. Pracownik potwierdza rozpoczęcie i zakończenie pracy zdalnej poprzez wysłanie sms-a lub e-maila z potwierdzeniem do Kierownika GOPS.

6. Wprowadza się regulamin pracy zdalnej, w brzmieniu załącznika do niniejszego zarządzenia.

§ 4. 1. Zarządzenie wchodzi w życie z dniem 30 marca 2020 roku.

2. Zarządzenie obowiązuje do dnia odwołania.

Kierownik Gminnego
Ośrodka Pomocy Społecznej

Justyna Kamińska

Załącznik do zarządzenia Nr 1/2020

Kierownika Gminnego Ośrodka Pomocy Społecznej

z dnia 27 marca 2020 r.

Regulamin pracy zdalnej

I. Wprowadzenie

1. Niniejszy regulamin określa zasady podejmowania i realizowania pracy zdalnej dla pracowników GOPS.

2. W Regulaminie pod określeniem "pracownik" należy rozumieć osoby zatrudnione w ramach stosunku pracy w GOPS.

II. Warunki podjęcia pracy zdalnej

1. W przypadku podjęcia pracy zdalnej pracownika obowiązują zasady pracy zdalnej określone w niniejszym Regulaminie.

2. Pracownik podejmując pracę zdalną zapewnia odpowiednie, zgodnie z niniejszym Regulaminem, warunki świadczenia tej pracy.

3. 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.

4. Złamanie zasad określonych w Regulaminie lub niedostosowanie się do postanowień niniejszego Regulaminu może stanowić naruszenie obowiązków pracowniczych.

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 oraz smartfona, a także zapewnienie pracy z dokumentami w sposób uniemożliwiający wgląd.

4. Odchodząc od komputera lub kończąc korzystanie ze służbowego smartfona należy upewnić się, że urządzenie zostało zablokowane.

IV. Bezpieczeństwo pracy zdalnej

Internet

1. 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,

5) został zmieniony domyślny adres routera (najczęściej 192.168.1.1.) na inny.

2. Porad i wsparcia w zakresie konfiguracji sieci domowej, w tym jej zabezpieczenia na potrzeby pracy zdalnej udziela informatyk Urzędu Gminy w Warlubiu.

Urządzenia służące do pracy zdalnej

1. Zabronione jest udostępnianie urządzeń wykorzystywanych do realizowania pracy zdalnej innym osobom, np. domownikom.

2. Urządzenie służbowe jest wydawane pracownikowi za protokołem.

3. Po otrzymaniu zgody na pracę zdalną, pracownik otrzymuje zaszyfrowany pendrive.

4. Pracownik zobowiązany jest do pracy na pendrive, bez kopiowaniu jakichkolwiek plików poza pendriva.

5. Minimalne wymagania w zakresie bezpieczeństwa:

1) na urządzeniu jest legalne i aktualne oprogramowanie,

2) zostały włączone automatyczne aktualizacje,

3) została włączona zapora systemowa,

4) został zainstalowany i działa w tle program antywirusowy,

5) zalogowanie do systemu operacyjnego wymaga uwierzytelnienia, np. poprzez indywidualny login i hasło użytkownika, kod PIN, token,

6) wyłączono autouzupełnianie i zapamiętywanie hasła w przeglądarce internetowej,

7) został zainstalowany program umożliwiający zaszyfrowanie i odszyfrowanie danych (np. 7-zip),

8) zostało ustawione automatyczne blokowanie urządzenia po dłuższym braku aktywności,

9) jeżeli urządzenie daje taką możliwość, praca jest wykonywana na koncie z ograniczonymi uprawnieniami.

6. Pracodawca może dodatkowo wymagać, aby urządzenie wykorzystywane do pracy zdalnej zawierało inne zabezpieczenia, jak:

1) zaszyfrowany dysk,

2) wyłączone porty pamięci zewnętrznych,

3) oprogramowanie służące monitorowaniu wykonywania pracy przez pracownika, wykorzystywane zgodnie z wymaganiami przepisów prawa pracy.

Zabezpieczanie przekazywanych informacji

1. Jeżeli jest niezbędne przesłanie informacji o charakterze poufnym, w szczególności danych osobowych, powinny zostać one zabezpieczone hasłem.

2. Jeżeli informacje poufne 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, czy adresy e-mail.

4. Hasło powinno zostać przekazane odbiorcy inną drogą komunikacji.

5. Hasło powinno być odpowiednio skomplikowane i niesłownikowe.

6. Dozwolone jest ustalenie stałego hasła na komunikację z jednym odbiorcą.

7. Rekomendowane metody zabezpieczania hasłem:

1) nadanie hasła do pliku, w którym są dane osobowe,

2) zabezpieczenie pliku lub plików poprzez kompresję z zabezpieczeniem archiwum wynikowego hasłem.

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

9. 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.

10. Pracownik może także przekazywać pliki z informacjami chronionymi z wykorzystaniem udostępnionych przez pracodawcę serwerów sieciowych lub plików FTP.

11. Wykorzystywanie innych narzędzi do przesyłania i udostępniania plików (weTransfer, Google Drive, DropBoX) może odbywać się tylko za zgodą pracodawcy, po wcześniejszym zabezpieczeniu hasłem plików.

Zasady korzystania z dokumentów w formie papierowej

1. Zgodnie z obowiązującym u pracodawcy zasadami wszystkie dokumenty zawierające informacje poufne, w tym dane osobowe, powinny być przechowywane w szafach zamykanych na klucz w siedzibie pracodawcy.

2. Obowiązuje ogólny zakaz zabierania dokumentów lub ich kopii poza siedzibę pracodawcy.

3. Jeżeli do pracy zdalnej niezbędny jest dostęp do dokumentów papierowych, pracownik zgłasza do pracodawcy prośbę o możliwość ich skopiowania oraz zabrania do domu na czas wykonywania pracy zdalnej.

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. Po zakończeniu pracy, wszystkie dokumenty należy zwrócić pracodawcy, który weryfikuje ich kompletność.

V. Szczególne sytuacje

1. Problemy w działaniu udostępnionego sprzętu lub oprogramowania należy niezwłocznie zgłaszać do informatyka.

2. W przypadku zgubienia lub kradzieży sprzętu, dokumentów lub innych nośników informacji, należy niezwłocznie, w dniu zdarzenia zgłosić zdarzenie do pracodawcy, informatyka, a także inspektora ochrony danych.

VI. Działania niedozwolone

1. 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 Gminy w Warlubiu przeglądu urządzenia,

6) niszczenie dokumentów w domu,

7) dzielenie się informacjami poufnymi z innymi osobami, w szczególności domownikami,

8) samodzielne zniszczenie dokumentów w domu,

9) logowanie się na konto innego użytkownika,

10) zabranie dokumentów bez pisemnej lub elektronicznej zgody pracodawcy,

11) zabranie oryginałów dokumentów,

12) niezwrócenie dokumentów,

13) niepotwierdzenie z pracodawcą zakresu zwróconych danych.