BURMISTRZ
Bystrzycy Kłodzkiej

ZARZĄDZENIE NR 0050.177.2020

BURMISTRZA BYSTRZYCY KŁODZKIEJ

z dnia 13 lipca 2020 roku

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 (Dz. U. z 2020 r. poz. 374) w związku z art. 33 ust. 3 i 5 ustawy z dnia 8 marca 1990 r. o samorządzie gminnym (Dz. U. z 2020 r. poz. 713)

oraz art. 3^1 § 1 ustawy z dnia 26 czerwca 1974 r. Kodeks pracy (Dz. U. z 2019 r. poz. 1040),

zarządza się, co następuje:

§ 1

W celu zapobiegania, przeciwdziałania i zwalczania COVID-19 wprowadza się Regulamin pracy zdalnej w brzmieniu załącznika do niniejszego zarządzenia.

§ 2

Wykonanie Zarządzenia powierzam Sekretarzowi Gminy.

§ 3

Zarządzenie wchodzi w życie z dniem podpisania.

Radca Prawny
WWb/546
Monika Pałynko-Bielska

Burmistrz
Bystrzycy Kłodzkiej
Renata Surma

Załącznik:

Regulamin pracy zdalnej

Regulamin pracy zdalnej

I. Wprowadzenie

1. Niniejszy regulamin określa zasady podejmowania i realizowania pracy zdalnej.
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 wymagające dostępu do zasobów sprzętowych i informacyjnych organizacji. Pod określeniem "pracodawca" należy rozumieć zarówno pracodawcę, jak i zlecającego usługi. Pod określeniem „dział IT" należy rozumieć Informatycy Urzędu Miasta i Gminy Bystrzyca Kłodzka.

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 pracodawca, jednakże pracownik może także zaproponować własny harmonogram i zakres pracy, który będzie mógł realizować po uzyskaniu zgody pracodawcy.
4. W przypadku podjęcia pracy zdalnej pracownika obowiązują zasady pracy zdalnej określone w niniejszym Regulaminie oraz w przepisach prawa powszechnie obowiązującego.
5. Pracownik podejmując pracę zdalną zapewnia odpowiednie, zgodnie z niniejszym Regulaminem, warunki świadczenia tej pracy.
6. 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.
7. 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.
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. 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 należy upewnić się, że urządzenie zostało zablokowane.

IV. Bezpieczeństwo pracy zdalnej

Internet

1. Pracownik wykonuje pracę zdalną z wykorzystaniem urządzeń służbowych, tzn. otrzymanych od pracodawcy lub z wykorzystaniem sprzętu prywatnego.
2. 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. Jeśli to możliwe, należy zmienić login do panelu administracyjnego routera na własny;
   c. Dostęp do panelu administracyjnego routera jest możliwy wyłącznie z urządzeń znajdujących się w sieci domowej;
3. Porad i wsparcia w zakresie konfiguracji sieci domowej, w tym jej zabezpieczenia na potrzeby pracy zdalnej udziela dział IT.

Urządzenia służące do pracy zdalnej

1. Zabronione jest udostępnianie urządzeń wykorzystywanych do realizowania pracy zdalnej innym osobom, np. domownikom.
2. Praca zdalna powinna być realizowana z wykorzystaniem służbowego sprzętu, takiego jak: komputer stacjonarny, laptop, smartfon. Wskazane narzędzia do pracy zdalnej co do zasady zapewnia pracodawca. Wykonywanie pracy zdalnej może zostać polecone, jeżeli

pracownik ma umiejętności i możliwości techniczne oraz lokalowe do wykonywania takiej pracy i pozwala na to jej rodzaj.

3. Pracodawca dopuszcza wykorzystywanie sprzętu prywatnego pod warunkiem, że umożliwi to zachowanie tajemnic, poufności i ochronę danych osobowych, których ujawnienie mogłoby narazić pracodawcę na szkodę.
4. Wykorzystanie sprzętu prywatnego do pracy zdalnej wymaga zawarcia odrębnej umowy pomiędzy pracodawcą i pracownikiem, pod warunkiem spełnienia przez pracownika wymogów bezpieczeństwa. W przewidzianych prawem sytuacjach na mocy zawartej umowy możliwe jest wypłacenie ekwiwalentu pracownikowi, jeżeli praca nie mogła być świadczona na sprzęcie służbowym, a spełnione zostały przesłanki ustawowe w zakresie pracy zdalnej na sprzęcie prywatnym.
5. 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. W takim przypadku stosuje się postanowienia pkt 3 i 4.
6. Zgoda na pracę zdalną obejmuje zgodę na korzystanie ze służbowego sprzętu poza siedzibą pracodawcy.
7. Urządzenie służbowe jest wydawane pracownikowi za protokołem. Protokół sporządza dział IT.
8. Po otrzymaniu pisemnej zgody na pracę zdalną i uzgodnieniu z pracodawcą z jakich urządzeń będzie korzystał pracownik w celu jej zrealizowania, pracownik niezwłocznie zgłasza ten fakt do działu IT.
9. Dział IT odnotowuje, które urządzania są wykorzystywane przez pracownika do pracy zdalnej, jeżeli to niezbędne, przeprowadza ich przegląd.
10. W przypadku, gdy przegląd jest niemożliwy, pracownik na żądanie pracownika działu IT udostępnia urządzenie zdalnie (z wykorzystaniem zaproponowanego przez dział IT narzędzia), w celu dokonania jego zdalnego przeglądu.
11. Przegląd urządzeń prywatnych jest obowiązkowy.
12. 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.

12. Pracodawca może dodatkowo wymagać, aby urządzenie wykorzystywane do pracy zdalnej zawierało inne zabezpieczenia, jak:
    - Zaszyfrowany dysk
    - Wyłączone porty pamięci zewnętrznych

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. 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.

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 otrzymaniu zgody na piśmie lub w formie służbowej wiadomości e-mail, pracownik może sporządzić kopie niezbędnych dokumentów.
5. Zabronione jest zabieranie poza siedzibę pracodawcy oryginałów dokumentów.
6. Po skopiowaniu dokumentów pracownik przygotowuje ich zestawienie, zawierające informacje jakie dokumenty, w jakiej liczbie zostały skopiowane.
7. Informacja jest przekazywana pracodawcy.
8. Podczas przewożenia dokumentów do miejsca realizowania pracy zdalnej, należy zachować szczególną ostrożność, aby ich nie zgubić.
9. Praca z dokumentami nie może być wykonywana w miejscu publicznym.
10. 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 działu IT.
2. W przypadku zgubienia lub kradzieży sprzętu, dokumentów lub innych nośników informacji, należy niezwłocznie, w dniu zdarzenia zgłosić zdarzenie do pracodawcy, działu IT, a także Inspektora Ochrony Danych.

VI. Działania niedozwolone

1. Niedozwolone jest:

- Udostępnianie innym osobom danych służących do uwierzytelnienia do systemów i/lub usług;
- Przekazywanie informacji chronionych, w szczególności danych osobowych bez zabezpieczenia hasłem, w szczególności w treści wiadomości e-mail;
- Przekazywanie hasła do zabezpieczonych informacji tą samą drogą komunikacji, którą przekazywany jest zabezpieczony hasłem plik lub pliki;
- Korzystanie z urządzeń, które nie zostały zatwierdzone przez pracodawcę;
- Odmówienie pracownikowi działu IT przeglądu urządzenia;
- Udostępnianie służbowego sprzętu lub sprzętu wykorzystywanego do realizowania zadań służbowych innym osobom;
- Dzielenie się informacjami poufnymi z innymi osobami, np. z domownikami;
- Samodzielne zniszczenie dokumentów w domu;
- Logowanie się na konto innego użytkownika;
- Zabranie dokumentów bez pisemnej lub elektronicznej zgody pracodawcy;
- Zabranie oryginałów dokumentów;
- Niezwrócenie dokumentów;
- Niepotwierdzenie z pracodawcą zakresu zwróconych danych.