ZARZĄDZENIE NR 179/2020
BURMISTRZA STRYKOWA

z dnia 27 października 2020 r.

w sprawie określenia Regulaminu pracy zdalnej i zasad bezpieczeństwa danych w Urzędzie Miejskim w Strykowie w czasie 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 (Dz. U. z 2020 r. poz. 1842) , art. 33 ust. 3 i 5 ustawy z dnia 8 marca 1990 r. o samorządzie gminnym (Dz. U. z 2020 r. poz. 713 i 1378), 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) zarządza się, co następuje:

§ 1. Określa się Regulamin pracy zdalnej i zasad bezpieczeństwa danych w Urzędzie Miejskim w Strykowie w czasie zagrożenia epidemicznego, stanowiący załącznik do niniejszego zarządzenia.

§ 2. Zobowiązuje się wszystkich pracowników Urzędu Miejskiego w Strykowie do zapoznania się z treścią niniejszego zarządzenia i jego stosowania.

§ 3. Wykonanie zarządzenia powierza się Sekretarzowi Gminy Stryków.

Załącznik do zarządzenia Nr 179/2020

Burmistrza Strykowa

z dnia 27 października 2020 r.

Regulamin pracy zdalnej i zasad bezpieczeństwa danych w Urzędzie Miejskim w Strykowie w czasie zagrożenia epidemicznego

Rozdział 1.
Wprowadzenie

§ 1. Niniejszy Regulamin określa zasady podejmowania i realizowania pracy zdalnejw związku z ogłoszeniem stanu epidemicznego na terenie Rzeczypospolitej Polskiej oraz możliwym potencjalnym zagrożeniem dla zdrowia pracowników Urzędu Miejskiego w Strykowie wirusem SARS-CoV-2 a także w celu zapewnienia ciągłości realizacji zadań gminy i zapewnienia niezbędnej pomocy obywatelom.

§ 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.

Rozdział 2.
Warunki podjęcia pracy zdalnej. Bezpieczeństwo pracy.

§ 4. Za wyjątkiem zmian wprowadzonych niniejszym zarządzeniem, pracownik zobowiązany jest do pracy zgodnie z warunkami określonymi w:

1) w umowie o pracę,

2) w informacji do umowy o pracę,

3) w zakresie obowiązków,

4) zgodnie ze złożonymi oświadczeniami, znajdującymi się w aktach osobowych,

5) w Regulaminie Pracy Urzędu,

6) Regulaminie Organizacyjnym Urzędu,

7) w Polityce Ochrony Danych Osobowych.

§ 5. 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 wykonywanej pracy określa bezpośredni przełożony pracownika, 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.

5. 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 informatyka wyznaczonego u pracodawcy, czy spełnia on wymogi przewidziane Regulaminem.

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. Pracodawca w zakresie niezbędnym do wykonywania pracy zdalnej zapewnia pracownikowi dostęp do służbowej poczty e-mail, a w przypadkach uzasadnionych zakresem obowiązków lub stanowiskiem służbowym także możliwość programów dedykowanych.

§ 6. 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.

Rozdział 3.
Warunki jakie musi spełniać miejsce świadczenia pracy zdalnej

§ 7. 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.

§ 8. Odchodząc od komputera lub kończąc korzystanie ze służbowego smartfona tableta Ipada, należy upewnić się, że urządzenie zostało zablokowane.

Rozdział 4.
Czas pracy

§ 9. 1. W trakcie wykonywania pracy zdalnej pracownik pracuje w systemie czasu pracy wynikającym z regulaminu pracy lub obowiązującej go umowy o pracę, co oznacza, żepracownik jest dostępny i realizuje swoje działania w ustalonych godzinach.

2. Praca zdalna powinna być wykonywa w godzinach normalnej pracy, w których dany pracownik pracował w Urzędzie. Praca zdalna powinna być wykonywana od poniedziałku do piątku.

3. Pracownik, wykonując pracę zdalną, powinien przestrzegać przepisów o czasie pracy, a zwłaszcza dotyczących nieprzerwanego 11-godzinnego odpoczynku dobowego.

4. Pracownik zobowiązany jest, każdego dnia, poinformować pracodawcę mailowo o rozpoczęciu pracy zdalnej, najpóźniej do godz.9.00.

5. Informacja, o której mowa w punkcie 4 powinna zostać przekazana na adres e-mailowy pracownika prowadzącego w Urzędzie sprawy kadrowe: ewa.tomczak@strykow.pl.

6. Na podstawie informacji, o której mowa w punkcie 4, na liście obecności znajdującej się w siedzibie pracodawcy, pracownikowi wykonującemu pracę zdalną przypisany zostanie symbol Zd – praca zdalna.

Rozdział 5.
Bezpieczeństwo pracy zdalnej

§ 10. 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.

§ 11. 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) porad i wsparcia w zakresie konfiguracji sieci domowej, w tym jej zabezpieczenia na potrzeby pracy zdalnej udziela informatyk wyznaczony przez pracodawcę.

§ 12. W celu zapewnienia bezpiecznej pracy pracownik zobowiązuje się, w szczególności do:

1) zabezpieczenia stacji roboczej poprzez aktualne oprogramowanie antywirusowe,

2) posiadanie indywidualnego loginu dostępu do systemu,

3) zabezpieczenia komputera hasłem o dużej złożoności hasła konta Administratora komputera i konta użytkownika oraz pracowania na koncie z adekwatnym poziomem uprawnień,

4) nieodchodzenia od komputera przed jego uprzednim zablokowaniem,

5) 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,

6) nieudostępniania sprzętu innym osobom,

7) nieinstalowania oprogramowania niebezpiecznego i pochodzącego z niewiadomych źródeł,

8) 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),

9) zadbania o bezpieczeństwo urządzeń w sieci domowej (np. silne hasło do sieci WiFi oraz aktualizacje oprogramowania urządzeń),

10) korzystania ze stabilnego i wydajnego łącza internetowego,

11) korzystania z bezpiecznych kanałów dostępności do Internetu (np. unikanie „otwartych" kanałów dostępowych WiFi),

12) korzystania z aktualnej przeglądarki internetowej. Zalecana jest praca w przeglądarce w tzw. trybie incognito,

13) 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,

14) unikania przeglądania stron potencjalnie niebezpiecznych,

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

16) 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),

17) stosowanie się do wytycznych pracodawcy.

Rozdział 6.
Zabezpieczanie przekazywanych informacji

§ 13. Do pracy zdalnej pracownik powinien wykorzystywać tylko i wyłącznie służbowe programy i systemy udostępnione mu przez pracodawcę, w tym służbową skrzynkę pocztową e-mail.

§ 14. 1. Jeżeli jest niezbędne przesłanie informacji o charakterze poufnym, w szczególności danych osobowych, powinny zostać one zabezpieczone i zaszyfrowane 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.

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

2. 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.

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

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

Rozdział 7.
Zasady korzystania z dokumentów w formie papierowej

§ 16. 1. Jeżeli do pracy zdalnej niezbędny jest dostęp do dokumentów papierowych zawierających informacje stanowiące tajemnicę służbową, w tym dane osobowe, pracownik zgłasza do bezpośredniego przełożonego 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 bezpośredniemu przełożonemu.

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, szkoła, kawiarnia, restauracja, galeria handlowa, itp.)

8. Po zakończeniu pracy, wszystkie dokumenty należy zwrócić bezpośredniemu przełożonemu, który weryfikuje ich kompletność.

Rozdział 8.
Szczególne sytuacje

§ 17. 1. Problemy w działaniu sprzętu lub oprogramowania, wykorzystywanego do pracy zdalnej 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.

Rozdział 9.
Działania niedozwolone

§ 18. 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 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) logowanie się na konto innego użytkownika,

10) zabranie dokumentów bez pisemnej lub elektronicznej zgody,

11) zabranie oryginałów dokumentów,

12) niezwrócenie dokumentów,

13) niepotwierdzenie z bezpośrednim przełożonym zakresu zwróconych danych,

14) wykonywanie działań niezwiązanych z realizacją czynności służbowych, określonych w umowie o pracę i zakresie czynności (np. zakupy).