Zarządzenie Nr 31/2020
Burmistrza Miasta Radymna
z dnia 30 marca 2020 roku

w sprawie zasad organizacji pracy zdalnej

Na podstawie art. 3 ustawy z dnia 2 marca 2020 roku 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) oraz art. 3^1 § 1 ustawy z dnia 26 czerwca 1974 Kodeks pracy (Dz.U. z 2019 r. poz. 1040 z późn. zm.), zarządza się co następuje:

§ 1. W związku z zagrożeniem chorobą COVID-19 wprowadza się wykonywanie pracy w warunkach tzw. pracy zdalnej, na zasadach określonych w Regulaminie, stanowiącym załącznik do Zarządzenia.

§ 2. Wykonanie zarządzenia powierza się Sekretarzowi.

§ 3. Zarządzenie wchodzi w życie z dniem podpisania.

BURMISTRZ
Mieczysław Piziurny

Załącznik do
Zarządzenia Nr 31/2020
Burmistrza Miasta Radymna
z dnia 30 marca 2020 roku

REGULAMIN WYKONYWANIA PRACY ZDALNEJ PRZEZ PRACOWNIKÓW URZĘDU MIASTA RADYMNA

§ 1. 1. Regulamin wykonywania pracy zdalnej przez pracowników Urzędu, zwany dalej „regulaminem", ustala zasady organizacji procesu pracy w systemie zdalnym oraz związane z tym szczególne prawa i obowiązki pracodawcy i pracowników.
2. Pracownik, o którym mowa w § 2, przed przystąpieniem do pracy zostaje zapoznany z treścią niniejszego regulaminu, co potwierdza pisemnym oświadczeniem i zobowiązaniem do jego przestrzegania.

§ 2. Ilekroć w regulaminie jest mowa o:
1. Pracy zdalnej - należy przez to rozumieć pracę wykonywaną regularnie poza siedzibą Pracodawcy, z wykorzystaniem środków komunikacji elektronicznej w rozumieniu przepisów o świadczeniu usług drogą elektroniczną;
2. Pracodawcy – należy przez to rozumieć Urząd Miasta Radymna,
3. Urzędzie – należy przez to rozumieć Urząd Miasta Radymna;
4. Pracowniku pracującemu zdalnie – należy przez to rozumieć pracownika, który na podstawie polecenia wykonuje pracę zdalnie i przekazuje wyniki swojej pracy, w szczególności za pośrednictwem środków komunikacji elektronicznej,
5. Sprzęcie – należy przez to rozumieć urządzenia informatyczne wraz z oprogramowaniem oraz środki łączności, które są niezbędne pracownikowi do regularnego wykonywania pracy poza siedzibą pracodawcy.

§ 3. Po przeprowadzeniu uzgodnień pomiędzy pracownikiem a pracodawcą oraz zaopiniowaniu przez informatyka, przygotowane zostaje polecenie do świadczenia pracy spoza miejsca pracy, ze wskazaniem miejsca, oraz dokonywania odbioru i kontroli wykonywanej pracy przez bezpośredniego przełożonego. Ponadto dokument powinien zawierać parametry techniczne niezbędnego sprzętu, zakres eksploatacji, serwisu i ubezpieczenia sprzętu należącego do pracodawcy.

§ 4. Pracownik może świadczyć pracę zdalnie na zasadach określonych w rozdziale II b działu drugiego Kodeksu pracy.

§5. W każdym terminie pracodawca może wystąpić z wiążącym wnioskiem o zaprzestanie świadczenia przez pracownika pracy zdalnie spoza siedziby pracodawcy i przywrócenie poprzednich warunków wykonywania pracy.

§ 6. Pracodawca jest zobowiązany w szczególności do przekazywania odpowiedniego sprzętu i zakresu zadań pracownikowi, udzielania informacji merytorycznych oraz do zorganizowania procesu pracy w sposób umożliwiający przestrzeganie norm czasu pracy, a ponadto do:
a. dostarczenia pracownikowi niezbędnego sprzętu do użytkowania poza siedzibą na podstawie protokołu zdawczo-odbiorczego,
b. zapewnienia pomocy technicznej w siedzibie pracodawcy lub o ile jest to możliwe zdalnie za pośrednictwem rozwiązań teleinformatycznych i w miarę potrzeb przeszkolenia pracownika w zakresie obsługi powierzonego sprzętu,

c. poniesienia wszelkich kosztów związanych z ubezpieczeniem sprzętu, jego instalacją, serwisem, eksploatacją i konserwacją, chyba że pracodawca i pracownik postanowią inaczej.

§ 7. Pracownik jest zobowiązany do efektywnego wykonywania pracy zgodnie z treścią umowy o pracę i zakresem obowiązków, z uwzględnieniem przepisów prawa pracy oraz Regulaminu Pracy funkcjonującego u pracodawcy, a ponadto do:
a. pozostawania w stałym kontakcie z bezpośrednim przełożonym lub inną wyznaczoną przez niego osobą w ustalonych godzinach pracy,
b. przyjmowania do realizacji bieżących zadań zleconych przez przełożonego w ramach powierzonego zakresu obowiązków, w szczególności z wykorzystaniem środków komunikacji elektronicznej,
c. bieżącego informowania o wynikach swojej pracy w formie ustalonej z bezpośrednim przełożonym;
d. potwierdzania codziennej obecności w pracy poprzez wypełnianie i przekazywanie do pracodawcy oświadczenia drogą mailową,
e. wykorzystywania powierzonego przez Pracodawcę sprzętu wyłącznie do celów służbowych oraz należytej ochrony przed jego uszkodzeniem, kradzieżą, zniszczeniem oraz nieuprawniony użyciem;
f. wykorzystywania powierzonych materiałów biurowych i technicznych wyłącznie do celów służbowych i rozliczania się z ich faktycznego i celowego wykorzystania;
g. zabezpieczania danych i informacji dostępnych za pomocą powierzonego sprzętu;
h. osobistego stawiennictwa w siedzibie pracodawcy w razie uzasadnionych potrzeb pracodawcy także na wezwanie przełożonego;
i. gotowości do poddania się kontroli ze strony uprawnionych służb.

§ 8. 1. Czasem pracy jest czas, w którym pracownik pozostaje w dyspozycji Pracodawcy w wyznaczonym miejscu pracy, utrzymując kontakt za pośrednictwem telefonu lub innego środka łączności, uzgodnionego z bezpośrednim przełożonym.
2. Pracownik jest obowiązany przestrzegać ustalonego czasu pracy i wykorzystywać go w pełni na wykonywanie swoich obowiązków pracowniczych, mając na uwadze, że praca nie ma na celu sprawowania opieki nad dziećmi lub osobami starszymi.
3. Pracownicy pracują w podstawowym lub zadaniowym systemie czasu pracy, w okresach rozliczeniowych zgodnie z zapisami w Regulaminie Pracy.
4. Zadania powierzone pracownikowi są ustalone w sposób możliwy do wykonania w czasie obejmującym przeciętnie 8 godzin na dobę i 40 godzin na tydzień przy zachowaniu pięciodniowego tygodnia pracy, w godzinach ustalonych z Pracodawcą.

§ 9. 1. Pracodawca, za pośrednictwem Inspektora Ochrony Danych oraz Informatyka, określa zasady bezpieczeństwa informacji przekazywanych pracownikowi oraz przeprowadza, w miarę potrzeb, instruktaż i szkolenie w tym zakresie.
2. Dodatkowe zasady bezpieczeństwa informacji stanowią załącznik numer 3 niniejszego regulaminu. Postanowienia Polityki Bezpieczeństwa Informacji stosuje się odpowiednio.
3. Pracownik potwierdza na piśmie zapoznanie się z zasadami ochrony danych, określonymi w załączniku numer 3 niniejszego regulaminu oraz jest zobowiązany do ich przestrzegania.
4. Aby zapewnić ochronę sprzętu, instalacja wszelkiego oprogramowania na komputerze udostępnionym przez pracodawcę do wykonywania pracy musi być uprzednio zatwierdzona przez informatyka oraz odbywać się przy zastosowaniu stosownych umów licencyjnych.
5. Pracownik, dla własnego bezpieczeństwa oraz dla bezpieczeństwa zasobów Pracodawcy, ma obowiązek sprawować pieczę w zakresie zapewnienia poufności i integralności danych, w tym także danych znajdujących się na twardym dysku lub przeglądanych za pomocą udostępnionego komputera, tak aby nie zostały one przejęte przez osoby trzecie, bezpowrotnie utracone lub zmienione w sposób nieautoryzowany.

§10. 1. W uzasadnionych przypadkach, na podstawie zgody udzielonej przez Burmistrza, dopuszcza się możliwość wyniesienia przez Pracownika dokumentów na potrzeby realizowania pracy zdalnej.
2. Dokumenty, które nie zostały wprowadzone do systemu EZD, mogą zostać udostępnione wyłącznie w postaci kserokopii. Oryginały dokumentów muszą pozostać w siedzibie Urzędu.
3. Dokumenty, które zostały wprowadzone do systemu EZD, mogą zostać przekazane Pracownikowi w postaci oryginalnej.
4. Dokumenty są udostępniane na podstawie protokołu zdawczo-odbiorczego, którego wzór stanowi załącznik numer 4 do niniejszego regulaminu.

§ 11.1. Jeżeli praca jest wykonywana w domu pracownika, pracodawca realizuje wobec niego w zakresie wynikającym z rodzaju i warunków wykonywanej pracy, obowiązki określone w dziale dziesiątym Kodeksu Pracy, z wyłączeniem:
a. dbałości o bezpieczny i higieniczny stan pomieszczeń pracy i wyposażenia technicznego, a także o sprawność środków ochrony zbiorowej i ich stosowanie zgodnie z przeznaczeniem,
b. stosowania regulacji dotyczących bezpieczeństwa i higieny pracy przy budowie i przebudowie obiektów, w których praca jest świadczona,
c. zapewnienia pracownikowi odpowiednich urządzeń higieniczno-sanitarnych i środków higieny osobistej, o których mowa w art. 233 Kodeksu pracy.
2. Urządzenia elektryczne dostarczane przez Pracodawcę są bezpieczne w momencie dostawy. Aby utrzymać ten stan, pracownik powinien regularnie sprawdzać je pod kątem wszelkich defektów (np. uszkodzeń izolacji), a w przypadku jakichkolwiek wątpliwości dotyczących urządzeń, skontaktować się ze swoim przełożonym.
3. W celu zachowania przepisów i zasad BHP, w szczególności ergonomii pracy i eliminacji możliwych zagrożeń, pracownik powinien przy tworzeniu i zmianach organizacji stanowiska pracy uwzględnić wymagania BHP i przeciwpożarowe.
4. Pracownik, który uległ wypadkowi przy pracy, wypadkowi w drodze do lub z pracy, jeżeli stan jego zdrowia na to pozwala, powinien niezwłocznie poinformować o zdarzeniu swojego przełożonego. Zgłoszenia należy dokonać telefonicznie, a następnie potwierdzić pisemnie.

§12. Pracownik ponosi konsekwencje przechowywania i wykorzystywania w powierzonych mu środkach przetwarzania informacji (np. w komputerze) nielegalnego oprogramowania oraz materiałów i plików.

BURMISTRZ
Mieczysław Piziurny

Załącznik Nr 1 do Regulaminu Wykonywania Pracy Zdalnej
wprowadzonego Zarządzeniem Nr 31/2020 Burmistrza Miasta Radymna
z dnia 30 marca 2020 roku

OŚWIADCZENIE PRACOWNIKA

.....
(imię i nazwisko pracownika)

Oświadczam, że zapoznałem/am się z Polityką Bezpieczeństwa Danych Osobowych oraz Polityką Bezpieczeństwa Informacji, a także z powyższymi zasadami bezpieczeństwa informacji, w trybie pracy zdalnej tj. wykonywanej poza siedzibą pracodawcy.

.....
(data i podpis pracownika)

Załącznik Nr 2 do Regulaminu Wykonywania Pracy Zdalnej
wprowadzonego Zarządzeniem Nr 31/2020 Burmistrza Miasta Radymna
z dnia 30 marca 2020 roku

.....

Imię i nazwisko, stanowisko, referat

Pan/Pani.....

(imię i nazwisko pracownika)

.....

(stanowisko)

POLECENIE PRACY ZDALNEJ

Na podstawie art. 3 ustawy z dnia 2 marca 2020 roku 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 zarządzeniem Nr 31/2020 Burmistrza Miasta Radymna z dnia 31 marca 2020 roku, w sprawie zasad organizacji pracy zdalnej,

polecam Panu/Pani pracę zdalną, która ma być wykonywana

w.....przy ulicy.....

kontakt telefoniczny pod numerem telefonu.....

Wszystkie dotychczasowe obowiązki wynikające z umowy o pracę, poza osobistymi spotkaniami z klientami, będzie Pan/pani realizować przez okres
od.....do....., w miejscu wskazanym wyżej, korzystając z zapewnionych przez pracodawcę narzędzi pracy, w tym:

1.....

2.....

3.....

W tym okresie kontakt z pracodawcą powinien odbywać się za pomocą środków porozumiewania się na odległość, w szczególności poprzez maile, telefony.

W okresie świadczenia pracy zdalnej jest Pan/Pani zobowiązany/(-a) do ewidencjonowania godzin wykonywanej pracy i przekazania tej ewidencji pracodawcy niezwłocznie po zakończeniu każdego miesiąca.

.....

podpis pracodawcy

Przyjmuję do wiadomości i stosowania polecenie pracy zdalnej

.....

(data i podpis pracownika)

Załącznik Nr 3 do Regulaminu Wykonywania Pracy Zdalnej
wprowadzony Zarządzeniem Nr 31/2020 Burmistrza Miasta Radymna
z dnia 30 marca 2020 roku

ZASADY BEZPIECZEŃSTWA INFORMACJI PRZY WYKONYWANIU PRACY ZDALNEJ

POSTAWANOWIENIA OGÓLNE

1. Każdy pracownik Urzędu, w tym również wykonujący pracę w trybie pracy zdalnej jest zobowiązany do przestrzegania postanowień Polityki Bezpieczeństwa Danych Osobowych oraz Polityki Bezpieczeństwa Informacji.
2. Pracownik zobowiązany jest do wydzielenia i zabezpieczenia miejsca pracy w celu ochrony przetwarzanych informacji oraz powierzonego sprzętu przed dostępem osób postronnych lub zniszczeniem. W szczególności zobowiązany jest do ochrony danych osobowych oraz innych danych stanowiących tajemnicę służbową przed osobami postronnymi, w tym także osobami wspólnie z nim mieszkającymi. Odchodząc od stanowiska pracy, pracownik każdorazowo jest zobowiązany do blokowania urządzenia na którym pracuje.
3. Niedopuszczalne jest przetwarzanie w formie pracy zdalnej danych posiadających klauzulę niejawności „zastrzeżone" lub wyższą.
4. Informacje, niezależnie od nośnika, na którym zostały zapisane, przeznaczone do użytku służbowego (stanowiące własność Urzędu) mogą być wykorzystywane wyłącznie do celów związanych z wykonywaniem obowiązków służbowych.
5. Zabrania się wykorzystywania prywatnych kont pocztowy do prowadzenia spraw służbowych.
6. Pracownik ponosi odpowiedzialność za bezpieczeństwo i dostęp do powierzonego mu sprzętu oraz za jego prawidłową eksploatację.
7. Zabronione jest:
   7.1. przechowywanie na dyskach twardych komputerów oraz na dyskach sieciowych plików niezwiązanych z wykonywanymi obowiązkami służbowymi;
   7.2. przechowywanie w środkach przetwarzania informacji oprogramowania, utworów muzycznych i wideo oraz innych plików, których używanie może powodować naruszenie praw własności intelektualnej.

ZASADY KORZYSTANIA Z URZĄDZEŃ MOBILNYCH

1. Urządzenia mobilne można wykorzystywać wyłącznie do realizacji zadań służbowych.
2. Zabrania się instalowania dodatkowych aplikacji lub oprogramowania na komputerze służbowym. Wyłączne uprawnienie w tym zakresie posiada Informatyk Urzędu.
3. Urząd dopuszcza, aby dla wygody i bezpieczeństwa informacji użytkownicy urządzeń mobilnych stosowali zabezpieczenia biometryczne dostarczane przez producentów tych rozwiązań (np. czytnik linii papilarnych, rozpoznawanie twarzy, itp.). Zaznacza się, że:

3.1. Urząd nie ma statusu Administratora Danych Osobowych dla danych biometrycznych zbieranych przez urządzenia mobilne;

3.2. Dane biometryczne służące do zabezpieczenia urządzeń mobilnych, są podawane przez ich użytkowników dobrowolnie, a o celach i środkach tego przetwarzania decydują sami użytkownicy;

3.3. Zastosowanie zabezpieczeń biometrycznych, o których mowa powyżej nie zwalnia użytkownika ze stosowania zasad dot. haseł określonych w niniejszym dokumencie.

4. Bez względu na miejsce jego użytkowania urządzenie powinno być należycie zabezpieczone przed nieuprawnionym dostępem, kradzieżą, zniszczeniem oraz innymi działaniami, które mogą wpłynąć na jego bezpieczeństwo.

5. Za ochronę informacji oraz urządzenia, odpowiada prawnie i materialnie jego użytkownik.

5.1. Użytkownicy są zobowiązani do ograniczenia używania urządzeń w miejscach publicznych oraz do zachowania szczególnej ostrożności w celu zapobieżenia wyciekom informacji.

5.2. W razie zgubienia lub kradzieży urządzenia, użytkownik zobowiązany jest do natychmiastowego zgłoszenia incydentu bezpieczeństwa.

6. Urządzenia, tam gdzie jest to możliwe technologicznie, powinny być zabezpieczone hasłem, a w przypadku przechowywania na nich informacji wymagających szyfrowania - posiadać szyfrowaną partycję służącą do przechowywania informacji podlegających ochronie. Informacje powinny być zaszyfrowane w sposób uniemożliwiający ich bezpośrednie odczytanie przez osoby trzecie w przypadku utraty urządzenia.

7. Zdalny dostęp do zasobów sieci Urzędu realizowany jest przy wykorzystaniu szyfrowanego mechanizmu VPN (z wykorzystaniem rozwiązania dostępnego w ramach stosowanego w Urzędzie UTM).

8. W przypadku złamania lub naruszenia regulacji w zakresie bezpieczeństwa sprzętu mobilnego, bezpośredni przełożony winien odebrać użytkownikowi zgodę na wynoszenie komputera poza miejsce pracy. W szczególnie uzasadnionych przypadkach powinien rozważyć możliwość pociągnięcia użytkownika do odpowiedzialności dyscyplinarnej.

9. Niedopuszczalne jest wykorzystywanie urządzeń do celów komercyjnych, reklamowych i politycznych oraz rozpowszechniania treści i obrazów godzących w dobre imię Urzędu.

10. Korzystanie z publicznych lub domowych kanałów dostępu (niezabezpieczone sieci Wi-Fi, punkty dostępowe dla klientów sklepu/kawiarni itp.) w celu komunikacji z systemami informatycznymi Urzędu jest zabronione, chyba że komunikacja odbywa się za pomocą zaufanego szyfrowanego połączenia (np. połączenia VPN) oraz uprzednio została udzielona zgoda Informatyka .

11. W razie utracenia urządzenia mobilnego – bez względu na to, czy był on szyfrowany, czy też nie – użytkownik jest zobowiązany do poinformowania o tym Informatyka oraz swojego bezpośredniego przełożonego.

BEZPIECZNA POCZTA ELEKTRONICZNA

1. Zakazuje się wykorzystywania prywatnych adresów poczty elektronicznej w sprawach służbowych.
2. Obowiązuje zakaz zapisywania haseł do poczty elektronicznej przez przeglądarkę internetową.
3. Podczas wysyłania wiadomości należy zweryfikować poprawność adresów e-mail odbiorcy.
4. Bezpieczne logowanie do poczty elektronicznej:
   4.1. Jeśli logujesz się do swojego konta poprzez interfejs webmail, korzystając z przeglądarki internetowej, sprawdź jaki adres pojawia się w pasku adresu. Powinien rozpoczynać się https://.
   4.2. Sprawdź certyfikat bezpieczeństwa (należy kliknąć kłódkę tuż obok paska adresu – wtedy wyświetla się informacja czy połączenie jest szyfrowane).
   4.3. Nie otwieraj załącznika, jeśli nie jesteś pewien, kto wysłał do Ciebie wiadomość.
   4.4. Unikaj otwierania plików, które zawierają końcówkę: exe, .bat, .com, .lnk, .scr, .vbs, tar., jar. rar., zip.,
   4.5. Nie klikaj w linki od nieznanych nadawców, mogą zawierać przekierowanie do zainfekowanych stron.
   4.6. Nie odpowiadaj na wiadomości od podejrzanych nadawców.
   4.7. Jeśli uznasz wiadomość za niechcianą i podejrzaną, oznacz ją jako SPAM.
   4.8. Do każdego konta podawaj zawsze inne hasło.
5. Korespondencja elektroniczna:
   5.1. Pracownik, przesyłając informacje za pośrednictwem poczty elektronicznej ponosi odpowiedzialność za prawidłowe zaadresowanie wiadomości elektronicznej i przesłanie jej do uprawnionego odbiorcy.
   5.2. Zabrania się przesyłania za pośrednictwem poczty elektronicznej treści niezgodnych z obowiązującymi przepisami prawa, naruszających zasady współżycia społecznego oraz naruszających prawa własności intelektualnej innych osób.
   5.3. Zabrania się przesyłania do innych pracowników wiadomości o treści niezwiązanej z obowiązkami służbowymi, a w szczególności wiadomości elektronicznych zawierających m.in.: informacje o charakterze komercyjnym, niechciane lub niepotrzebne wiadomości.
   5.4. Zabrania się rozsyłania za pośrednictwem poczty elektronicznej załączników zawierających pliki zagrażające lub mogące zagrażać bezpieczeństwu systemu teleinformatycznego Urzędu.
   5.5. Zabrania się wykorzystywania przydzielonego pracownikowi konta pocztowego do celów prywatnych (np. prowadzenie korespondencji niezwiązanej z działalnością służbową, rejestrowania się przy jego użyciu na forach, portalach społecznościowych, newsletterach, itp.).
   5.6. Zabrania się przekierowywania poczty służbowej na prywatną skrzynkę (np. w celu pracy w domu).
   5.7. W ramach użytkowania poczty elektronicznej zabrania się wysyłania plików multimedialnych (np. .mp3, .wav, .mov, .avi) oraz wykonywalnych (np. exe, .bat, .com, .cmd), chyba że wynika to wprost z obowiązków służbowych wykonywanych przez pracownika.

OPROGRAMOWANIE

1. Pracownik może korzystać jedynie z oprogramowania, na które pracodawca posiada aktualne licencje lub posiada prawo do używania.
2. Pracownik nie może za pomocą komputerów służbowych pobierać z Internetu lub przesyłać nielicencjonowanego oprogramowania oraz innych utworów chronionych prawem autorskim (w tym w szczególności utworów muzycznych, filmów, grafiki, gier komputerowych i tym podobnych).
3. Pracownik nie może instalować na komputerach pracodawcy prywatnych kopii oprogramowania, plików muzycznych i video, z żadnego nośnika i z żadnego innego urządzenia.

ZASADY DOTYCZĄCE DOSTĘPU DO SIECI INTERNET

1. Dostęp do sieci Internet może odbywać się wyłącznie na podstawie nadanych uprawnień w zakresie realizowania zadań służbowych. Korzystając z usług sieciowych należy przestrzegać następujących zasad:
   1.1. użytkować Internet wyłącznie do celów służbowych,
   1.2. korzystać wyłącznie z witryn internetowych niezbędnych do realizacji zadań służbowych,
   1.3. zweryfikować certyfikaty udostępniane na witrynie,
   1.4. pliki zawierające dane chronione należy przed wysłaniem zabezpieczyć (stosując szyfrowanie wiadomości z hasłem do otwarcia pliku).
2. Korzystanie z sieci Internet:
   2.1. Pracownik ma prawo korzystać z sieci Internet wyłącznie w celach związanych z realizacją zadań służbowych, zgodnie z obowiązującymi regulaminami i przepisami prawa, w zakresie przyznanych uprawnień.
   2.2. Zabronione jest korzystanie z sieci Internet w celu uzyskania nieuprawnionego dostępu do zasobów będących własnością Urzędu lub zasobów podmiotów zewnętrznych, pobierania, udostępniania i rozpowszechniania jakichkolwiek materiałów (informacji, danych, tekstów, programów komputerowych, dźwięków, fotografii, grafik, filmów) naruszających prawa własności intelektualnej, pobierania, udostępniania i rozpowszechniania jakichkolwiek materiałów zakazanych przepisami prawa, w tym m.in. zawierających groźby, treści obraźliwe, zniesławiające, pornograficzne lub naruszających w jakikolwiek inny sposób prawa innych osób.
   2.3. Zabronione jest podejmowanie przez pracowników działań powodujących istotne ograniczenia w korzystaniu z sieci Internet przez innych pracowników, a w szczególności: pobieranie dużej ilości danych, w sytuacji, gdy nie jest to uzasadnione wykonywanymi obowiązkami służbowymi, podejmowanie działań skutkujących ograniczeniami w funkcjonowaniu jakichkolwiek usług sieciowych.
   2.4. Z wyłączeniem Informatyka, zabronione jest umożliwianie przez pracowników Urzędu dostępu z Internetu do zasobów zlokalizowanych na urządzeniu komputerowym (np. przy wykorzystaniu serwerów WWW, ftp, programów tunelujących, P2P).

ZASADY DOTYCZĄCE POLITYKI ANTYWIRUSOWEJ

14.1. W przypadku, gdy program antywirusowy zgłasza nieaktualną bazę sygnatur wirusów należy o tym fakcie poinformować Informatyka telefonicznie lub na adres e-mail: informatyk@radymno.pl

14.2. W przypadku identyfikacji wirusa na komputerze należy zawiesić pracę i niezwłocznie o tym fakcie poinformować Informatyka telefonicznie lub na adres e-mail: informatyk@radymno.pl

14.3. Wszystkie nośniki zewnętrzne podłączane do stacji roboczej należy przed użyciem sprawdzić programem antywirusowym.

ZGŁASZANIE ZDARZEŃ MOGĄCYCH ŚWIADCZYĆ O NARUSZENIU BEZPIECZEŃSTWA

14.4. Wszystkie niestandardowe działania systemu informatycznego oraz zdarzenia mogące wskazywać na utratę bezpieczeństwa powinny być niezwłocznie zgłoszone do Informatyka telefonicznie oraz na adres e-mail: informatyk@radymno.pl

14.5. Symptomy wskazujące, na możliwość naruszenia bezpieczeństwa teleinformatycznego:

- obcy identyfikator w oknie logowania,
- nietypowe obciążenie (spowolnienie pracy) stacji roboczej,
- nowe oprogramowanie nieznanego typu,
- wyłączony program antywirusowy,
- zwiększona ilość niechcianej poczty (spamu),
- brak możliwości zalogowania się na własny identyfikator i hasło,
- nazwy plików w historii, które nie były otwierane,
- użytkowania przez osoby trzecie w czasie nieobecności pracownika.

BURMISTRZ
Mieczysław Pizłurny

Załącznik Nr 4 do Regulaminu Wykonywania Pracy Zdalnej
wprowadzonego Zarządzeniem Nr 31/2020 W Burmistrza Miasta Radymna
z dnia 30 marca 2020 roku

PROTOKÓŁ ZDAWCZO-ODBIORCZY DOKUMENTÓW

Miejscowość	Radymno
Przekazujący dokumenty	Kierownik Komórki Organizacyjnej
Przyjmujący dokumenty	Pracownik, który pobiera dokumenty do pracy zdalnej
Spis przekazywanych dokumentów	
Uzasadnienie	Proszę uzasadnić dlaczego nie da się pracować na dokumencie elektronicznym
Akceptacja …	
Data przekazania dokumentów	
Potwierdzenie kompletności zwracanych dokumentów	Potwierdzam / nie potwierdzam
Data zdania dokumentów	
Data i podpis przekazującego	
Data i podpis przyjmującego	