Zarządzenie Nr 6/2020
Dyrektora Publicznego Przedszkola w Jemielnicy
Z dnia 16.03.2020

w sprawie wprowadzenia Regulaminu pracy zdalnej w Publicznym Przedszkolu w Jemielnicy

W związku ze szczególną sytuacją spowodowaną epidemią koronawirusa i w związku z tym ograniczeniem funkcjonowania podmiotów systemu oświaty

Na podstawie:

- Ustawy z dnia 14 grudnia 2016 r. Prawo oświatowe(Dz.U. z 11.01.2017 r. poz. 59),
- Ustawy z dnia 7 września 1991r. o systemie oświaty (Dz. U. z 2019 r. poz. 1481, 1818 i 2197),
- Rozporządzenia MEN z dnia 11 marca 2020 w sprawie czasowego ograniczenia funkcjonowania jednostek systemu oświaty w związku z zapobieganiem, przeciwdziałaniem i zwalczaniem COVID-19.
- Rozporządzenia MEN z dnia 20 marca 2020 zmieniającego rozporządzenie w sprawie czasowego ograniczenia funkcjonowania jednostek systemu oświaty w związku z zapobieganiem, przeciwdziałaniem i zwalczaniem COVID-19

Dyrektor Publicznego Przedszkola w Jemielnicy zarządza:

§1

Wprowadzenie Regulaminu Pracy zdalnej w Publicznym Przedszkolu w Jemielnicy, który stanowi załącznik do niniejszego zarządzenia.

§2

Zobowiązuję wszystkich pracowników Publicznego Przedszkola w Jemielnicy do zapoznania z treścią Regulaminu (załącznik 1).

§3

Za prawidłowe wdrożenie w życie postanowień Regulaminu pracy zdalnej odpowiedzialni są wszyscy pracownicy, każdy w swoim zakresie.

§4

Zarządzenie wchodzi w życie z dniem podpisania.

Załącznik 1

REGULAMIN PRACY ZDALNEJ

SPIS TREŚCI:

I. WPROWADZENIE

1. Niniejszy regulamin określa zasady podejmowania i realizowania pracy zdalnej.
2. Niniejszy regulamin ma zastosowanie w każdym miejscu wykonywania pracy lub polecenia administratora.
3. Niniejszy regulamin nie wyklucza stosowania panujących polityk np. ochrony danych, bezpieczeństwa informacji, bezpieczeństwa i higieny pracy oraz innych wynikających z przepisów, a jedynie je uzupełnia.

II. DEFINICJE

1. Poniższe definicje mają zastosowanie do całego Regulaminu Pracy Zdalnej wraz z załącznikami:
   a. **Administrator** – lub pracodawca
   b. **Regulamin** – niniejszy regulamin pracy zdalnej.
   c. **Praca zdalna** – należy przez to rozumieć pracę określoną w umowie o pracę, umowie zlecenie, umowie o współpracy oraz innej umowie cywilnoprawnej łączącej Pracownika z Pracodawcą, wykonywaną przez czas oznaczony poza miejscem jej stałego wykonywania, jeżeli wykonywanie pracy poza takim miejscem jest możliwe.
   d. **Pracownik** – należy przez to rozumieć osobę zatrudnioną w oparciu o umowę o pracę oraz inną umowę cywilnoprawną, w tym umowę zlecenie, umowę o współpracy, umowę o dzieło, jeśli realizacja tej umowy wiąże się z wykonywaniem obowiązków na rzecz Pracodawcy w miejscu ich stałego wykonywania wyznaczonym przez Pracodawcę.
   e. **Ustawa** – należy przez to rozumieć ustawę 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. 2020 poz. 374 z późn. zm.).
   f. **Naruszenie bezpieczeństwa** – przypadkowe lub niezgodne z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych lub danych poufnych przesyłanych, przechowywanych lub w inny sposób przetwarzanych oraz wszelakie awarie urządzeń, systemów, aplikacji i programów wykorzystywanych do pracy zdalnej.

III. OBOWIĄZKI ADMINISTRATORA

1. Administrator odpowiada za ustalenie minimalnych wymagań bezpieczeństwa informacji podczas pracy zdalnej i może nie udzielić zgody na jej wykonywanie, jeżeli nie będzie można tych wymagań zagwarantować.
2. Administrator odpowiada za prowadzenie **ewidencji urządzeń służbowych wykorzystywanych do pracy zdalnej** oraz **ewidencji udostępnionej dokumentacji**.
3. W przypadku oddelegowania pracownika do pracy zdalnej administrator zobowiązuje się do:
   a. przekazania Pracownikowi zadań do wykonania;
   b. udzielenia Pracownikowi wszystkich ważnych informacji merytorycznych;
   c. zorganizowania procesu pracy zdalnej w sposób umożliwiający Pracownikowi wykonywanie pracy.

IV. OBOWIĄZKI PRACOWNIKA

1. Pracownik jest zobowiązany do wykonywania pracy zdalnej zgodnie z:
   a. treścią umowy łączącej go z Pracodawcą;
   b. zakresem obowiązków;

c. panującymi politykami bezpieczeństwa informacji;
d. poleceniem Administratora;
e. niniejszym regulaminem.

2. Ponadto Pracownik zobowiązuje się do:
   a. pozostawania dyspozycyjnym dla Pracodawcy w ustalonych godzinach pracy;
   b. przyjmowania do realizacji bieżących zadań przekazywanych Pracownikowi w ramach zakresu jego obowiązków, w szczególności z wykorzystaniem środków komunikacji elektronicznej;
   c. bieżącego informowania o wynikach swojej pracy oraz przedstawiania wyników swojej pracy Pracodawcy;
   d. potwierdzania obecności w pracy w sposób określony przez Pracodawcę;
   e. zorganizowania stanowiska do pracy zdalnej w sposób zapewniający bezpieczne i higieniczne warunki pracy.

V. ZASADY BEZPIECZEŃSTWA

1. Pracownik wykonujący pracę zdalną zobowiązany jest do przestrzegania następujących zasad:
   a. należy blokować komputer przy wyjściu na każdą przerwę (choćby "tylko na chwilę"). W windows umożliwia to skrót klawiaturowy Win+L, w macOS: control+command+Q;
   b. należy używać odpowiednio złożonych haseł dostępowych (obecnie cztery-pięć względnie losowo dobranych słów stanowi solidne hasło);
   c. należy korzystać z managerów haseł;
   d. należy zamykać komputer po zakończonej pracy (pamiętaj o "zamykaniu" nie "usypianiu" czy "hibernowaniu");
   e. należy w miarę możliwości zadbać o osobny pokój do pracy lub wydzielenie odpowiedniej przestrzeni, tak aby ewentualne osoby postronne, nie miały dostępu do dokumentów poufnych lub zawierających dane osobowe;
   f. należy podjąć szczególne środki bezpieczeństwa, aby urządzenia wykorzystywane do pracy zdalnej, szczególnie te wykorzystywane do przenoszenia danych, jak dyski zewnętrzne nie zostały zgubione, zniszczone lub udostępnione;
   g. należy zwrócić wszystkie pobrane dokumenty do siedziby administratora i uzyskać potwierdzenie zwrotu i zakresu zwróconych dokumentów;
   h. należy bezwzględnie stosować politykę czystego biurka, ekranu i pulpitu.
2. Pracownik wykonujący pracę zdalną zobowiązany jest do przestrzegania poniższych zakazów:
   a. zakaz udostępniania innym osobom danych służących do uwierzytelnienia do systemów i/lub usług;
   b. zakaz przekazywania informacji poufnych, w szczególności danych osobowych bez zabezpieczenia hasłem, w szczególności w treści wiadomości e-mail;
   c. zakaz przekazywania hasła do zabezpieczonych informacji tą samą drogą komunikacji, którą przekazywany jest zabezpieczony hasłem plik lub pliki;
   d. zakaz korzystania z urządzeń, które nie zostały zatwierdzone przez pracodawcę;
   e. zakaz niszczenia dokumentów w domu;
   f. zakaz udostępniania służbowego sprzętu lub sprzętu wykorzystywanego do realizowania zadań służbowych innym osobom;
   g. zakaz dzielenia się informacjami poufnymi z innymi osobami, w szczególności domownikami;
   h. zakaz logowania na konto innego użytkownika;
   i. zakaz zabierania dokumentów bez pisemnej lub elektronicznej zgody pracodawcy;
   j. zakaz zabierania oryginałów dokumentów.

VI. ROZPOCZĘCIE PRACY ZDALNEJ

1. O możliwości podjęcia pracy zdalnej przez pracownika decyduje Administrator.
2. Pracownik może zgłosić administratorowi chęć podjęcia pracy zdalnej.
3. Warunki i zasady pracy zdalnej, w tym zakres i harmonogram wykonywanej pracy określa administrator.
4. Pracownik może zaproponować własny harmonogram i zakres pracy, który będzie mógł realizować po uzyskaniu zgody administratora.
5. W przypadku podjęcia pracy zdalnej pracownik zobowiązany jest niezwłocznie:
   a. zapoznać się z niniejszym regulaminem;
   b. podpisać i dostarczyć załącznik **„Oświadczenie"** administratorowi;
   c. postępować zgodnie z niniejszym regulaminem.
6. Pracownik podejmując pracę zdalną zapewnia odpowiednie, zgodnie z niniejszym Regulaminem warunki świadczenia tej pracy.
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.

VII. MIEJSCE WYKONYWANIA PRACY ZDALNEJ

1. Pracownik musi zapewnić właściwe warunki umożliwiające mu skuteczną pracę zdalną, a w szczególności właściwy poziom bezpieczeństwa informacji w miejscu wykonywania pracy zdalnej.
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:
    a. ustawienie ekranu komputera oraz smartfona w sposób uniemożliwiający wgląd;
    b. przechowywanie dokumentacji w sposób uniemożliwiający wgląd lub zniszczenie;
    c. pracowanie na dokumentacji w sposób uniemożliwiający wgląd lub zniszczenie;
    d. odchodząc od komputera lub kończąc korzystanie ze służbowego smartfona należy upewnić się, że urządzenie zostało zablokowane.
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.

VIII. URZĄDZENIA WYKORZYSTYWANE 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 jak komputer stacjonarny, laptop, smartfon, tablet, itp.
3. Zgoda na pracę zdalną obejmuje zgodę na korzystanie ze służbowego sprzętu poza siedzibą pracodawcy.
4. Pracownik jest uprawniony także do zabrania komputera stacjonarnego do miejsca wykonywania pracy zdalnej, na czas wykonywania tej pracy.
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.
6. Urządzenie służbowe jest wydawane pracownikowi z protokołem.
7. Po otrzymaniu 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.
8. Dział IT odnotowuje w załączniku „ewidencja urządzeń wykorzystywanych do pracy zdalnej", które urządzenia są wykorzystywane przez pracownika do pracy zdalnej, jeżeli to niezbędne, przeprowadza ich przegląd.
9. 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.
10. Przegląd urządzeń prywatnych jest obowiązkowy.
11. Minimalne wymagania w zakresie bezpieczeństwa:
    a. Na urządzeniu jest legalne i aktualne oprogramowanie.
    b. Zostały włączone automatyczne aktualizacje.
    c. Została włączona zapora systemowa.
    d. Został zainstalowany i działa w tle program antywirusowy.
    e. Zalogowanie do systemu operacyjnego wymaga uwierzytelnienia, np. poprzez indywidualny login i hasło użytkownika, kod PIN, token.
    f. Wyłączono autouzupełnianie i zapamiętywanie hasła w przeglądarce internetowej.
    g. Został zainstalowany program umożliwiający zaszyfrowanie i odszyfrowanie danych (np. 7-zip).
    h. Zostało ustawione automatyczne blokowanie urządzenia po dłuższym braku aktywności.
    i. 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:
    a. Zaszyfrowany dysk.
    b. Wyłączone porty pamięci zewnętrznych.
    c. Oprogramowanie służące monitorowaniu wykonywania pracy przez pracownika, wykorzystywane zgodnie z wymaganiami przepisów prawa pracy.

IX. DOKUMENTY W FORMIE PAPIEROWEJ

1. Zgodnie z obowiązującymi u Administratora 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. Informacja jest przekazywana pracodawcy.
7. Podczas przewożenia dokumentów do miejsca realizowania pracy zdalnej należy zachować szczególną ostrożność, aby ich nie zgubić, nie zniszczyć lub nie ujawnić ich treści.
8. Praca z dokumentami nie może być wykonywana w miejscu publicznym (świetlica w szkole, kawiarnia, restauracja, galeria handlowa itp.).
9. Po zakończeniu pracy wszystkie dokumenty należy zwrócić pracodawcy, który weryfikuje ich

kompletność.

X. INTERNET

1. Zabronione jest korzystanie z otwartych sieci Wifi.
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.

XI. PRZEKAZYWANIE INFORMACJI

1. Do przekazywania informacji Pracownik może wykorzystywać tylko i wyłącznie służbowe programy i systemy udostępnione mu przez administratora.
2. Jeżeli jest niezbędne przesłanie informacji o charakterze poufnym, muszą zostać one zabezpieczone hasłem.
3. Zabezpieczone hasłem muszą także zawsze być wszelkiego rodzaju dokumenty zawierające 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. Wykorzystywanie innych narzędzi niż poczta e-mail do przesyłania i udostępniania plików (weTransfer, Google Drive, DropBoX) może odbywać się tylko za zgodą pracodawcy i po wcześniejszym zabezpieczeniu hasłem plików.

XII. POCZTA E-MAIL

1. Należy używać jedynie służbowych kont e-mail, chyba że administrator wyraził zgodę na wykorzystanie innego konta i inspektor danych osobowych nie miał żadnych przeciwwskazań.
2. Wysyłając dane poufne lub dane osobowe wykorzystując konto e-mail należy się upewnić, że:
   a. treści wiadomości i załączniki są właściwie szyfrowane i zabezpieczone hasłem;
   b. w temacie wiadomości nie ma informacji poufnych lub danych osobowych;
   c. wiadomość wysyłana jest do właściwego adresata;
   d. w przypadku wysyłania informacji do kilku odbiorców, którzy nie znają się wzajemnie i/lub ich adresy
      e-mail są adresami prywatnymi, adresaci wprowadzeni są w pole UDW
3. Odbierając widomości e-mail należy:
   a. sprawdzić dokładnie nadawcę e-maila;
   b. nie otwierać wiadomości, załączników, linków od nieznanych nadawców;
   c. usuwać lub przenosić do SPAM wiadomości z nieznanego źródła.

XIII. NARUSZENIE BEZPIECZEŃSTWA

1. Każdy pracownik, który zaobserwuje, że doszło do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, ujawnienia, udostępnienia danych osobowych lub innych danych poufnych ma obowiązek sporządzić notatkę ze zdarzenia na podstawie załącznika „**Notatka ze zdarzenia**" i niezwłocznie przesłać ją do administratora, działu IT i inspektora ochrony danych.
2. Każdy pracownik, który zaobserwuje, że doszło do awarii urządzenia, systemu, aplikacji lub programu ma obowiązek niezwłocznie poinformować o tym dział IT i działać zgodnie z wytycznymi.
3. W przypadku zgubienia lub kradzieży sprzętu, dokumentów lub innych nośników informacji, należy niezwłocznie, w dniu zdarzenia zgłosić zdarzenie do pracodawcy, działu IT i inspektora ochrony danych.

XIV. KONTROLE

1. Następujące osoby we wskazanych zakresach mogą dokonywać kontroli:
   a. administrator – w każdym zakresie;
   b. inspektor ochrony danych – w zakresie bezpieczeństwa przetwarzanych danych osobowych;
   c. dział IT – w zakresie bezpieczeństwa informacji przetwarzanych w systemach, aplikacjach i programach;
   d. audytor wewnętrzny – w zakresie zgodności z prawem;
   e. inspektor BHP – w zakresie bezpieczeństwa i higieny pracy.
2. Pracownik nie może utrudniać kontroli kontrolującemu, musi wykonywać jego polecenia i wspierać go w przeprowadzanej kontroli.
3. Kontrolujący ma prawo:
   a. wglądu do danych poufnych w zakresie niezbędnym do przeprowadzenia kontroli;
   b. żądać od kontrolowanego wyjaśnień, informacji, dokumentów niezbędnych do prowadzenia

kontroli;
c. nakazać pracownikowi w określonym terminie uregulować wykryte uchybienia;
d. zakazać dalszej pracy pracownikowi, jeżeli wykryte zostało wysokie ryzyko naruszenia bezpieczeństwa.

XV. POSTANOWIENIA KOŃCOWE

1. Niniejszy regulamin obowiązuje od 16.03.2020.
2. Regulamin zostaje wprowadzony zarządzeniem numer 6/2020 z dnia 16.03.2020.
3. Regulamin zostaje udostępniony wszystkim pracownikom wykonującym pracę zdalną oraz na stronie Przedszkola.
4. Zmiany regulaminu mogą zostać wprowadzone jedynie zarządzeniem administratora.

Zapoznałem/am się z Regulaminem Pracy Zdalnej w Publicznym Przedszkolu w Jemielnicy

Lp.	Nazwisko i imię	Data	Podpis
1			
2			
3			
4			
5			
6			
7			
8			
9			
10			
11			
12			
13			
14			
15			
16			
17			
18			
19			
20			
21			
22			

23			
24			
25			
26			
27			
28			
29			
30			