

ZARZĄDZENIE Nr GZOPO.0210.2.6.2020
Dyrektora Gminnego Zespołu Obsługi Placówek Oświatowych w Świerklanach
z dnia 8 kwietnia 2020 r.

**w sprawie ustalenia Regulaminu pracy zdalnej w Gminnym Zespole Obsługi Placówek
Oświatowych w Świerklanach**

Na podstawie art. 47 ustawy z dnia 8 marca 1990 r. o samorządzie gminnym (tj. Dz. U. z 2019 r., poz. 506 z późn. zm.) oraz 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 2020r. poz.374 ze zmianami)

zarządzam, co następuje:

§ 1

Ustalić Regulamin pracy zdalnej w Gminnym Zespole Obsługi Placówek Oświatowych w Świerklanach stanowiącym załącznik do niniejszego zarządzenia.

§ 2

Treść zarządzenia podaje się do wiadomości pracowników.

§ 3

Zarządzenie wchodzi w życie z dniem podpisania.

Podpisał:
Dyrektor Gminnego Zespołu Obsługi Placówek
Oświatowych
w Świerklanach
Kamil Gąsior

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. Pod określeniem "pracodawca" należy rozumieć zarówno pracodawcę, jak i zlecającego usługi.

II. Warunki podjęcia pracy zdalnej

1. O możliwości podjęcia pracy zdalnej przez pracownika decyduje pracodawca w formie polecenia zgodnie z wzorem stanowiącym załącznik nr 1 do niniejszego zarządzenia.
2. Pracownik może zgłosić pracodawcy chęć podjęcia pracy zdalnej, jeżeli nie został do niej zobowiązany.
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.
5. Pracodawca ma prawo kontrolować wykonywanie pracy zdalnej oraz żądać od pracownika i bezpośredniego przełożonego informacji o jej wynikach.
6. Pracownik podejmując pracę zdalną zapewnia odpowiednie, zgodnie z niniejszym Regulaminem, warunki świadczenia tej pracy.
7. Pracownik wykonuje pracę zdalną w miejscu zamieszkania lub innym miejscu uzgodnionym z Pracodawcą. Pracownik jest zobowiązany do wykonywania pracy zgodnie z treścią umowy łączącej go z Pracodawcą oraz zakresem obowiązków.
8. Pracownik zobowiązuje się do bieżącego informowania o wynikach swojej pracy oraz przedstawiania wyników swojej pracy Dyrektorowi GZOPO.
9. 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.
10. Złamanie zasad określonych w Regulaminie lub niedostosowanie się do postanowień niniejszego Regulaminu może stanowić naruszenie obowiązków pracowniczych.
11. Pracownik w formie oświadczenia stanowiącym załącznik nr 2 do niniejszego Regulaminu, akceptuje zasady pracy zdalnej w GZOPO w Świerklanach.

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. 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 wykonując pracę zdalną z wykorzystaniem urządzeń służbowych, tzn. otrzymanych od pracodawcy, lub własnych, w przypadku na brak sprzętu służbowego
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:
 - Korzystanie z Internetu powinno wymagać uwierzytelnienia, np. poprzez hasło, ponadto urządzenie powinno mieć możliwość wybrania opcji szyfrowania połączenia WIFI za pomocą protokołu WPA2,
 - Hasło dostępu powinno składać się z co najmniej 10 znaków, w tym z dużych i małych liter oraz cyfr i znaków specjalnych.
 - Jeśli to możliwe, należy zmienić login do panelu administracyjnego routera na własny.
 - Dostęp do panelu administracyjnego routera jest możliwy wyłącznie z urządzeń znajdujących się w sieci domowej.
 - Został zmieniony domyślny adres routera (najczęściej 192.168.1.1.) na inny.
4. Porad i wsparcia w zakresie konfiguracji sieci domowej, w tym jej zabezpieczenia na potrzeby pracy zdalnej udziela ASI.

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, jak komputera stacjonarny, laptop, smartfon, tablet, itp., lub własnego, w przypadku braku urządzeń służbowych.
3. Zgoda na pracę zdalną obejmuje zgodę na korzystanie ze służbowego sprzętu poza siedzibą pracodawcy oraz przetwarzania danych osobowych poza budynkiem jednostki organizacyjnej.
5. Jeżeli z jakichś 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 za 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 ASI.
8. ASI odnotowuje, 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 ASI udostępnia urządzenie zdalnie (z wykorzystaniem zaproponowanego przez ASI narzędzia), w celu dokonania jego zdalnego przeglądu.
10. Przegląd urządzeń prywatnych jest obowiązkowy.
11. Minimalne wymagania w zakresie bezpieczeństwa:
 - Na urządzeniu jest legalne i aktualne oprogramowanie,
 - Zostały włączone automatyczne aktualizacje,
 - Została włączona zapor systemowa,
 - Został zainstalowany i działa w tle program antywirusowy,

- Zalogowanie do systemu operacyjnego wymaga uwierzytelnienia, np. poprzez indywidualny login i hasło użytkownika,
 - 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,
 - Oprogramowanie służące monitorowaniu wykonywania pracy przez pracownika, wykorzystywane zgodnie z wymaganiami przepisów prawa pracy,
 - Inne określone przez ASI.

Zabezpieczanie przekazywanych informacji

1. Do pracy zdalnej pracownik powinien wykorzystywać tylko i wyłącznie służbowe programy i systemy udostępnione mu przez pracodawcę, lub własne w przypadku braku możliwości udostępnienia ich 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 – np. sms.
6. Hasło powinno być odpowiednio skomplikowane i niesłownikowe.
7. Dozwolone jest ustalenie stałego hasła na komunikację z jednym odbiorcą.
8. 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.
12. Każda wiadomość powinna być wysyłana z należytą starannością, polegającą w szczególności na sprawdzeniu, czy jest kierowana do odpowiedniego odbiorcy.
13. 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.
14. Pracownik może także przekazywać pliki z informacjami chronionymi z wykorzystaniem udostępnionych przez pracodawcę serwerów sieciowych lub plików FTP.
15. 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. Zasady zabezpieczenia ich w domu są takie same jak w przypadku wymagań określonych w punkcie 1.

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 (kawiarnia, restauracja, galeria handlowa, itp.)
10. Po zakończeniu pracy, wszystkie dokumenty należy zwrócić pracodawcy, który weryfikuje ich kompletność.
11. Pracodawca może zezwolić na udostępnianie dokumentów pracownikowi realizującemu pracę zdalną drogą elektroniczną.

V. Szczególne sytuacje

1. Problemy w działaniu udostępnionego sprzętu lub oprogramowania należy niezwłocznie zgłaszać ASI.
2. W przypadku zgubienia lub kradzieży sprzętu, dokumentów lub innych nośników informacji, należy niezwłocznie, w dniu zdarzenia zgłosić zdarzenie do pracodawcy, ASI, 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 ASI przeglądu urządzenia;
 - Udostępnianie służbowego sprzętu lub sprzętu wykorzystywanego do realizowania zadań służbowych innym osobom;
 - Dzielenie się informacjami poufnymi z innymi osobami, w szczególności 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.

Podpisał:
Dyrektor Gminnego Zespołu Obsługi Placówek
Oświatowych
w Świerklanach
Kamil Gąsior

Świerklany, dnia

.....
(Imię i nazwisko pracownika)

.....
(stanowisko)

Polecenie pracy zdalnej

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, zobowiązuje Panią/a do podjęcia pracy w okresie od do w celu wykonywania obowiązków służbowych poza miejscem pracy tj. w miejscu zamieszkania.

Przy wykonywaniu pracy zdalnej jest Pani/Pan zobowiązany do realizowania obowiązków służbowych określonych w Pani/Pana zakresie obowiązków służbowych.

W czasie wykonywania pracy zdalnej nie ulegają zmianie obowiązujące Panią/Pana godziny rozpoczęcia i zakończenia pracy, a także przepisy i regulacje wewnątrzzakładowe dotyczące przerw w pracy.

Ponadto informuję, iż:

- Podczas wykonywania pracy zdalnej jest Pani/Pan zobowiązana/y do przestrzegania przepisów o ochronie danych osobowych, a także dbania o bezpieczne przetwarzanie przez Panią/Pana powierzonych danych, bez dostępu do nich osób nieupoważnionych, zgodnie z wewnątrzzakładowymi procedurami.
- Pouczam Panią/Pana o obowiązku wykonywania pracy przy zachowaniu bezpiecznych i higienicznych warunków pracy w zakresie zasad pracy na stanowiskach wyposażonych w monitory ekranowe.

.....
(czytelny podpis)

Przyjmuję pracę zdalną ww. okresie:

.....
(podpis pracownika)

Świerklany, dnia

.....
(Imię i nazwisko pracownika)

.....
(stanowisko)

Oświadczenie

W związku z podjęciem pracy zdalnej, że:

1. Wyrażam zgodę na świadczenie pracy zdalnej na moim prywatnym sprzęcie komputerowym.
2. Oświadczam, że:
 - Dane pracodawcy zachowam w poufności.
 - Pracować będę na komputerze własnym, na którym zainstalowany jest aktualny system operacyjny Windows 8 lub 10, do którego posiadam prawa licencyjne.
 - Komputer chroniony jest aktualnym programem/systemem antywirusowym do którego posiadam prawa licencyjne.
 - Korzystam z sieci internetowej zabezpieczonej hasłem dostępowym, do której nie posiadają dostępu osoby postronne.
 - Przestrzegać będę polityk bezpieczeństwa wdrożonych przez pracodawcę oraz zasadach bezpieczeństwa dla pracy zdalnej, o których mnie poinformowano (*Regulamin pracy zdalnej w Gminnym Zespole Obsługi Placówek Oświatowych w Świerklanach dołączony do oświadczenia*).

Jednocześnie Oświadczam, że znane są mi zasady ochrony danych osobowych oraz zasady pracy zdalnej przyjętej Zarządzeniem Dyrektora GZOPO nr GZOPO.0210.2.6.2020 z dnia 8 kwietnia 2020 roku **w sprawie ustalenia Regulaminu pracy zdalnej w Gminnym Zespole Obsługi Placówek Oświatowych w Świerklanach.**

.....
(czytelny podpis)