

Regulamin pracy zdalnej w Zespole Szkół Centrum Kształcenia Ustawicznego w Sulejowie

Spis treści

I. Postanowienia ogólne.....	1
II. Warunki podjęcia pracy zdalnej.....	1
III. Wymogi wobec miejsca świadczenia pracy zdalnej.....	2
IV. Warunki bezpieczeństwa pracy zdalnej.....	2
V. Zasady korzystania z dokumentów w formie papierowej.....	4
VI. Zasady bezpieczeństwa przy prowadzeniu wideokonferencji.....	5
VII. Szczególne sytuacje.....	5
VIII. Działania niedozwolone.....	6

I. Postanowienia ogólne

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 stałe 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.

II. Warunki podjęcia pracy zdalnej

3. O możliwości podjęcia pracy zdalnej przez pracownika decyduje pracodawca.
4. Pracownik może zgłosić pracodawcy chęć podjęcia pracy zdalnej.
5. 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.

6. W przypadku podjęcia pracy zdalnej pracownika obowiązują zasady pracy zdalnej określone w niniejszym Regulaminie.
7. Pracownik podejmując pracę zdalną zapewnia odpowiednie, zgodnie z niniejszym Regulaminem, warunki świadczenia tej pracy.
8. Jeżeli pracownik nie ma możliwości świadczenia pracy zdalnej z zapewnieniem właściwych zabezpieczeń, w szczególności ze względu na siłę wyższą (np. brak zasilania w energię elektryczną; dostępu do Internetu), niezwłocznie zgłasza to pracodawcy i postępuje zgodnie z jego instrukcjami.
9. 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. Wymogi wobec miejsca świadczenia pracy zdalnej

10. Pracownik musi zapewnić właściwe warunki umożliwiające mu skuteczną pracę zdalną z zachowaniem właściwego poziomu bezpieczeństwa informacji.
11. Niedozwolone jest podejmowanie pracy zdalnej w miejscach publicznych, gdzie osoby postronne mogłyby usłyszeć fragmenty służbowych rozmów lub zapoznać się z fragmentami wykonywanej pracy.
12. Pracując w domu należy tak zorganizować stanowisko pracy, aby domownicy nie mieli wglądu w wykonywaną pracę, w szczególności poprzez właściwe ustawienie ekranu komputera, a także zapewnienie pracy z dokumentami w sposób uniemożliwiający do nich wgląd.
13. Praca zdalna powinna odbywać się zgodnie z harmonogramem ustalonym z pracodawcą, co oznacza, że pracownik jest dostępny i realizuje swoje działania w ustalonych godzinach.
14. Odchodząc od komputera lub kończąc korzystanie ze służbowego smartfona należy upewnić się, że urządzenie zostało zablokowane.

IV. Warunki bezpieczeństwa pracy zdalnej

Prace przez Internet

1. Pracownik wykonuje pracę zdalną z wykorzystaniem urządzeń służbowych, tzn. otrzymanych od pracodawcy.
2. W przypadku korzystania z domowej sieci WiFi, należy upewnić się, że została ona skonfigurowana w sposób minimalizujący ryzyko włamania, a 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 winien być 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 pracownik właściwy do spraw 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, jak komputera 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 za pokwitowaniem.
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 pracownika właściwego do spraw IT.
8. Pracownik właściwy do spraw IT 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 pracownika właściwego do spraw IT udostępnia urządzenie zdalnie (z wykorzystaniem zaproponowanego przez dział IT narzędzia), w celu dokonania jego zdalnego przeglądu.
10. Minimalne wymagania w zakresie bezpieczeństwa pracy na sprzęcie prywatnym:
 - a. na urządzeniu jest zainstalowane legalne i aktualne oprogramowanie
 - b. zostały włączone automatyczne aktualizacje
 - c. została włączona zapor systemowa
 - d. został zainstalowany i działa w tle program antywirusowy
 - e. zalogowanie do systemu operacyjnego wymaga uwierzytelnienia, np. poprzez indywidualny login i hasło użytkownika,
 - 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
11. Pracownik składa pisemne oświadczenie, że jego prywatny sprzęt wykorzystywany do pracy zdalnej spełnia wymagania określone powyżej.

Zabezpieczanie przekazywanych informacji

1. Do pracy zdalnej pracownik powinien wykorzystywać tylko i wyłącznie służbowe programy i systemy udostępnione mu przez pracodawcę.
2. Do prowadzenia korespondencji należy wykorzystywać wyłącznie adresy poczty elektronicznej przypisane pracownikowi przez pracodawcę.
3. Jeżeli jest niezbędne przesłanie informacji o charakterze poufnym, w szczególności danych osobowych, powinny zostać one zabezpieczone hasłem.
4. Jeżeli informacje poufne będą przekazywane z wykorzystaniem poczty e-mail, powinny zostać udostępnione w załączniku zabezpieczonym hasłem.
5. Zabezpieczeniu powinny podlegać wszelkiego rodzaju dane osobowe, niezależnie od ich charakteru.
6. Hasło powinno zostać przekazane odbiorcy inną drogą komunikacji.
7. Hasło powinno być odpowiednio skomplikowane i niesłownikowe.
8. Dozwolone jest ustalenie stałego hasła na komunikację z jednym odbiorcą.
9. 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.
10. Każda wiadomość powinna być wysyłana z należytą starannością, polegającą w szczególności na sprawdzeniu, czy jest kierowana do odpowiedniego odbiorcy.
11. 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.

V. Zasady korzystania z dokumentów w formie papierowej

15. 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.
16. Obowiązuje ogólny zakaz zabierania dokumentów lub ich kopii poza siedzibę pracodawcy.
17. 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.
18. Po otrzymaniu zgody na piśmie lub w formie służbowej wiadomości e-mail, pracownik może sporządzić kopie niezbędnych dokumentów.
19. Zabronione jest zabieranie poza siedzibę pracodawcy oryginałów dokumentów.
20. Po skopiowaniu dokumentów pracownik przygotowuje ich zestawienie, zawierające informacje jakie dokumenty, w jakiej liczbie zostały skopiowane.
21. Informacja jest przekazywana pracodawcy.
22. Podczas przewożenia dokumentów do miejsca realizowania pracy zdalnej, należy zachować szczególną ostrożność, aby ich nie utracić.
23. Praca z dokumentami nie może być wykonywana w miejscu publicznym.

24. Po zakończeniu pracy, wszystkie dokumenty należy zwrócić pracodawcy, który weryfikuje ich kompletność.

VI. Zasady bezpieczeństwa przy prowadzeniu wideokonferencji

25. Wideokonferencje prowadzi się z wykorzystaniem narzędzi informatycznych autoryzowanych i udostępnionych przez pracodawcę

26. Uczestnicząc w wideokonferencjach należy zadbać, aby obszar objęty wideo transmisją (w szczególności za uczestnikiem) zapewniał prywatność uczestnika. Należy w tym zakresie dobrać ustawienie kamery tak aby obszar za uczestnikiem stanowiła ściana lub jednolite tło, nienaruszające jego prywatności. W przypadku gdy system informatyczny to umożliwia należy skorzystać z opcji automatycznego zamazywania lub podmiany tła.

27. Odchodząc od miejsca wideokonferencji należy się z niej rozłączyć lub wyłączyć mikrofon i kamerę na czas nieobecności lub prowadzenia rozmowy prywatnej.

28. Nagrywanie wideokonferencji musi być prawnie uzasadnione i nie może naruszać prywatności uczestników wideokonferencji.

29. Prowadzący wideokonferencje informuje o jej nagrywaniu jej uczestników przed rozpoczęciem nagrywania.

30. W przypadku konieczności udostępnienia pulpitu innym uczestnikom wideokonferencji należy upewnić się, że nie zostaną udostępnione w ten sposób informacje podlegające szczególnej ochronie oraz że wszyscy uczestnicy konferencji uprawnieni są do dostępu do prezentowanych treści.

31. W ramach wideokonferencji mogą być udostępniane innym uczestnikom pliki, jednakże wyłącznie w zakresie autoryzowanego przez pracodawcę narzędzia do prowadzenia wideokonferencji.

VII. Szczególne sytuacje

32. Problemy w działaniu udostępnionego sprzętu lub oprogramowania należy niezwłocznie zgłaszać do pracownika IT.

33. W przypadku zgubienia lub kradzieży sprzętu, dokumentów lub innych nośników informacji, a także stwierdzenia lub podejrzenia innego naruszenia bezpieczeństwa informacji w tym w szczególności danych osobowych należy niezwłocznie, w dniu zdarzenia zgłosić zdarzenie do pracodawcy, a także inspektora ochrony danych.

VIII. Działania niedozwolone

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 pracownikowi IT przeglądu urządzenia;
6. Niszczanie 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. Zabieranie dokumentów bez zgody pracodawcy;
11. Zabieranie oryginałów dokumentów;
12. Niezwrócenie dokumentów;
13. Niepotwierdzenie z pracodawcą zakresu zwróconych danych.

DYREKTOR SZKOŁY
mgr inż. Stanisław Ból