

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, jak i współpracowników, na stałe wykonujących zadania w ramach umów cywilnoprawnych wymagające dostępu do zasobów sprzętowych i informacyjnych organizacji.

II. Warunki podjęcia pracy zdalnej

1. O możliwości podjęcia pracy zdalnej przez pracownika decyduje dyrektor.
2. Pracownik może zgłosić dyrektorowi chęć podjęcia pracy zdalnej.
3. Warunki i zasady pracy zdalnej, w tym zakres i harmonogram wykonywanej pracy określa dyrektor, jednakże pracownik może także zaproponować własny harmonogram i zakres pracy, który będzie mógł realizować po uzyskaniu zgody dyrektora.
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.
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 dyrektorowi i prowadzi pracę zdalną w budynku szkoły.
7. Złamanie zasad określonych w Regulaminie lub niedostosowanie się do postanowień niniejszego Regulaminu może stanowić naruszenie obowiązków pracowniczych.

III. Warunki jakie musi spełniać miejsce świadczenia pracy zdalnej

1. Pracownik musi zapewnić że ma 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 dyrektorem, 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 wykonuje pracę zdalną z wykorzystaniem urządzeń służbowych, tzn. otrzymanych ze szkoły lub prywatnych.
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:
 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. Został zmieniony domyślny adres routera (najczęściej 192.168.1.1.) na inny.

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 własnego lub służbowego sprzętu, jak komputera stacjonarny, laptop, smartfon, tablet, itp.
3. Zgoda na pracę zdalną obejmuje zgodę na korzystanie z własnego lub służbowego sprzętu poza siedzibą pracodawcy.
4. Pracownik jest uprawniony także do zabrania komputera stacjonarnego (laptopa) do miejsca wykonywania pracy zdalnej, na czas wykonywania tej pracy.
5. Urządzenie służbowe jest wydawane pracownikowi za protokołem.
6. Po otrzymaniu zgody na pracę zdalną i uzgodnieniu z pracodawcą z jakich urządzeń będzie korzystał pracownik w celu jej zrealizowania, pracownik niezwłocznie zgłasza to w sekretariacie szkoły.
7. Pani Sekretarka odnotowuje, które urządzenia są wykorzystywane przez pracownika do pracy zdalnej, jeżeli to niezbędne, przeprowadza ich przegląd.
8. Przegląd urządzeń prywatnych jest obowiązkowy.
9. Minimalne wymagania w zakresie bezpieczeństwa:
 - Na urządzeniu jest legalne i aktualne oprogramowanie
 - Zostały włączone automatyczne aktualizacje
 - Została włączona zapora systemowa
 - Został zainstalowany i działa w tle program antywirusowy
 - Zalogowanie do systemu operacyjnego wymaga uwierzytelnienia, np. poprzez indywidualny login i hasło użytkownika, kod PIN, token
 - 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

Zabezpieczanie przekazywanych informacji

1. Do pracy zdalnej pracownik powinien wykorzystywać tylko i wyłącznie służbowe programy i systemy udostępnione mu przez szkołę.
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.
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.
9. Każda wiadomość powinna być wysyłana z należytą starannością, polegającą w szczególności na sprawdzeniu, czy jest kierowana do odpowiedniego odbiorcy.
10. 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.
11. 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 szkole.
2. Obowiązuje ogólny zakaz zabierania dokumentów lub ich kopii poza siedzibę szkoły.
3. Jeżeli do pracy zdalnej niezbędny jest dostęp do dokumentów papierowych, pracownik zgłasza do dyrektora 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 szkolne oryginałów dokumentów.
6. Po skopiowaniu dokumentów pracownik przygotowuje ich zestawienie, zawierające informacje jakie dokumenty, w jakiej liczbie zostały skopiowane.
7. Informacja jest przekazywana dyrektorowi.
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 (świetlica w szkole, kawiarnia, restauracja, galeria handlowa, itp.)
10. Po zakończeniu pracy, wszystkie dokumenty należy zwrócić dyrektorowi, który weryfikuje ich kompletność.

V. Szczególne sytuacje

1. Problemy w działaniu udostępnionego sprzętu lub oprogramowania należy niezwłocznie zgłaszać do pana Tomasza Podleńskiego.
2. W przypadku zgubienia lub kradzieży sprzętu, dokumentów lub innych nośników informacji, należy niezwłocznie, w dniu zdarzenia zgłosić zdarzenie do dyrektora oraz inspektorowi danych osobowych pani Iwonie Baście.

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 pracownikowi działu IT przeglądu urządzenia;
 - Niszczenie dokumentów w domu;
 - 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.