REGULAMIN PRACY ZDALNEJ

w

Zespole Szkół Ogólnokształcących im. Pawła Stalmacha w Wiśle

Postanowienia wstępne

§ 1.

1. Regulamin określa zasady podejmowania i realizowania pracy zdalnej.
2. W Regulaminie przez "pracownika" należy rozumieć zarówno nauczycieli, jak i pracowników niepedagogicznych zatrudnionych w Zespole Szkół Ogólnokształcących im. Pawła Stalmacha w Wiśle

Warunki pracy zdalnej

§ 2.

1. możliwości podjęcia pracy zdalnej przez pracownika decyduje pracodawca.
2. Pracownik może zgłosić pracodawcy chęć podjęcia pracy zdalnej. Zgoda na pracę zdalną obejmuje zgodę na korzystanie ze służbowego sprzętu poza siedzibą pracodawcy lub własnego sprzętu.
3. Warunki i zasady pracy zdalnej określa pracodawca, jednakże pracownik może także zaproponować własny harmonogram i zakres pracy, który będzie mógł realizować po uzyskaniu zgody pracodawcy.

§ 3.

1. W przypadku podjęcia pracy zdalnej pracownika obowiązują zasady pracy zdalnej określone w niniejszym Regulaminie.

§ 4.

1. Pracownik podejmując pracę zdalną zapewnia odpowiednie warunki świadczenia tej pracy 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 laptopa/komputera/tabletu/smartfona, a także zapewnienie pracy z dokumentami w sposób uniemożliwiający wgląd.
4. Pracownik jest dostępny i realizuje swoje działania w ustalonych godzinach.
5. 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 (np. telefonicznie) i postępuje zgodnie z jego instrukcjami.

Urządzenia służące do pracy zdalnej

§ 5.

1. Pracownik wykonuję pracę zdalną z wykorzystaniem urządzeń otrzymanych od pracodawcy lub na własnym sprzęcie.
2. Pracownik jest uprawniony, za zgodą pracodawcy, do zabrania komputera stacjonarnego do miejsca wykonywania pracy zdalnej, na czas wykonywania tej pracy.
3. Zabronione jest udostępnianie urządzeń wykorzystywanych do realizowania pracy zdalnej innym osobom, np. domownikom.

§ 6.

1. Urządzenie służbowe jest wydawane pracownikowi za protokołem.
2. Pracodawca może zezwolić pracownikowi na korzystanie z prywatnych urządzeń, pod warunkiem zapewnienia minimalnych wymagań w zakresie bezpieczeństwa.
3. Minimalne wymagania w zakresie bezpieczeństwa:

1) na urządzeniu jest legalne i aktualne oprogramowanie,

2) zostały włączone automatyczne aktualizacje,
3) została włączona zapora systemowa,
4) został zainstalowany i działa w tle program antywirusowy,
5) zalogowanie do systemu operacyjnego wymaga uwierzytelnienia, np. poprzez indywidualny login i hasło użytkownika, kod PIN,
6) wyłączono autouzupełnianie i zapamiętywanie hasła w przeglądarce internetowej,
7) zostało ustawione automatyczne blokowanie urządzenia po dłuższym braku aktywności,

4. Problemy w działaniu udostępnionego sprzętu lub oprogramowania należy niezwłocznie zgłaszać do pracodawcy.
5. W przypadku zgubienia lub kradzieży sprzętu należy niezwłocznie, w dniu zdarzenia zgłosić zdarzenie do pracodawcy, a także inspektora ochrony danych.

Bezpieczeństwo informatyczne

§ 7.

1. Pracownik w przypadku korzystania z domowej sieci WiFi, musi upewnić się, że została ona skonfigurowana w sposób minimalizujący ryzyko włamania, w szczególności:

1) korzystanie z Internetu powinno wymagać uwierzytelnienia, np. poprzez hasło,
2) dostęp do panelu administracyjnego routera jest możliwy wyłącznie z urządzeń znajdujących się w sieci domowej.

2. Porad i wsparcia w zakresie konfiguracji sieci domowej, w tym jej zabezpieczenia na potrzeby pracy zdalnej udzielą nauczyciele informatyki pracujący w ZSO w Wiśle.

Zabezpieczanie przekazywanych danych osobowych lub informacji

§ 8.

1. Jeżeli jest niezbędne przesłanie informacji o charakterze poufnym, w szczególności danych osobowych, powinny zostać one zabezpieczone hasłem.
2. Jeżeli informacje poufne będą przekazywane z wykorzystaniem poczty e-mail, powinny zostać udostępnione w załączniku zabezpieczonym hasłem.

3. Zabezpieczeniu powinny podlegać wszelkiego rodzaju dane osobowe, niezależnie od ich charakteru.

§ 9.

1. Hasło powinno zostać przekazane odbiorcy inną drogą komunikacji.
2. Hasło powinno być odpowiednio skomplikowane. Dozwolone jest ustalenie stałego hasła na komunikację z jednym odbiorcą.
3. Rekomendowane metody zabezpieczania hasłem:

1) nadanie hasła do pliku, w którym są dane osobowe
2) zabezpieczenie pliku lub plików poprzez kompresję z zabezpieczeniem archiwum hasłem.

§ 10.

1. Każda wiadomość powinna być wysyłana z należytą starannością, polegającą w szczególności na sprawdzeniu, czy jest kierowana do odpowiedniego odbiorcy.
2. 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), tzn. adresy wpisać w to pole.

Korzystanie z dokumentów w formie papierowej poza siedzibą pracodawcy

§ 11.

1. 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.
2. Po otrzymaniu zgody na piśmie lub w formie służbowej wiadomości e-mail, pracownik może sporządzić kopie niezbędnych dokumentów.
3. Po skopiowaniu dokumentów pracownik przygotowuje ich zestawienie dla pracodawcy, zawierające informacje jakie dokumenty, w jakiej liczbie zostały skopiowane.
4. Po zakończeniu pracy, wszystkie dokumenty należy zwrócić pracodawcy, który weryfikuje ich kompletność.

§ 12.

1. Zabronione jest zabieranie poza siedzibę pracodawcy oryginałów dokumentów.

§ 13.

1. W przypadku zgubienia lub kradzieży dokumentów lub innych nośników informacji, należy niezwłocznie, w dniu zdarzenia zgłosić zdarzenie do pracodawcy, a także inspektora ochrony danych.

Działania nieprawidłowe

§ 14.

1. Niedozwolone jest:
1) udostępnianie innym osobom danych służących do uwierzytelnienia do systemów,
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 spełniają minimalnych wymagań w zakresie bezpieczeństwa określonych w § 6 ust. 5;
5) niszczenie dokumentów w domu;
6) udostępnianie służbowego sprzętu lub sprzętu wykorzystywanego do realizowania zadań służbowych innym osobom;
7) dzielenie się informacjami poufnymi z innymi osobami, w szczególności domownikami;
8) zabranie dokumentów bez pisemnej lub elektronicznej zgody pracodawcy;
9) zabranie oryginałów dokumentów;
10) niezwrócenie dokumentów;
11) niepotwierdzenie z pracodawcą zakresu zwróconych danych.

Postanowienia końcowe

§ 15.

Złamanie zasad określonych w Regulaminie lub niedostosowanie się do postanowień niniejszego Regulaminu może stanowić naruszenie obowiązków pracowniczych.