

Zarządzenie nr 107/20
Rektora Państwowej Wyższej Szkoły Zawodowej im. Witelona w Legnicy
z dnia 21 października 2020 r.

w sprawie wprowadzenia zasad bezpieczeństwa pracy zdalnej obowiązujące w Państwowej Wyższej Szkole Zawodowej im. Witelona w Legnicy

Na podstawie art. 23 ustawy z dnia 20 lipca 2018 r. Prawo o szkolnictwie wyższym i nauce (Dz.U. z 2020 r. poz. 85 z późn.zm.) zarządzam, co następuje:

§ 1.

Wprowadzam zasady bezpieczeństwa pracy zdalnej obowiązujące w Państwowej Wyższej Szkole Zawodowej im. Witelona w Legnicy.

§ 2.

Zarządzenie wchodzi w życie z dniem podpisania.


REKTOR
dr hab. Andrzej Panasiuk

**Zasady bezpieczeństwa pracy zdalnej obowiązujące w Państwowej Wyższej Szkole Zawodowej im.
Witelona w Legnicy**

§ 1.

Wprowadzenie

1. Praca zdalna jest rozwiązaniem systemowym wprowadzonym na czas określony w związku z przeciwdziałaniem Covid-19, polegającym na świadczeniu pracy poza siedzibą Państwowej Wyższej Szkoły Zawodowej im. Witelona w Legnicy, zwanej dalej Uczelnią.
2. Decyzje w sprawie wyrażania zgody na pracę zdalną, bądź polecenia świadczenia takiej pracy podejmuje odpowiednio kierownik jednostki lub komórki organizacyjnej.
3. Osoba świadcząca pracę zdalną może zostać zobowiązana do złożenia raportów z realizacji swoich obowiązków.
4. Miejscem wykonywania pracy zdalnej i korzystania ze sprzętu jest miejsce zamieszkania lub inne uzgodnione miejsce.

§ 2.

Bezpieczeństwo pracy zdalnej

1. Wykonywanie pracy zdalnej nie zwalnia z obowiązku przestrzegania przepisów dotyczących ochrony danych osobowych przyjętych w Uczelni.
2. Miejsce świadczenia pracy zdalnej powinno być zabezpieczone w taki sposób, aby zapobiegać przed zniszczeniem danych, oraz żeby osoby postronne nie miały do nich dostępu oraz do informacji w formie elektronicznej oraz papierowej.
3. Odchodząc od komputera należy upewnić się, że urządzenie zostało zablokowane.
4. W przypadku korzystania z domowej sieci WiFi, należy upewnić się, że została ona skonfigurowana w sposób minimalizujący ryzyko włamania, w szczególności:
 - 1) połączenie z domową siecią WiFi 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) jeżeli jest to możliwe, należy zmienić login do panelu administracyjnego routera na własny;
 - 4) dostęp do panelu administracyjnego routera powinien być możliwy wyłącznie z urządzeń znajdujących się w sieci domowej;
 - 5) gdy został zmieniony domyślny adres routera (najczęściej 192.168.1.1.) na inny.
5. Pomocy w zakresie konfiguracji sieci domowej, w tym jej zabezpieczenia, na potrzeby pracy zdalnej, udziela Sekcja ds. Informatyzacji.

§ 3.

Urządzenia służące do pracy zdalnej

1. Praca zdalna powinna być wykonywana przede wszystkim z wykorzystaniem urządzeń służbowych, takich jak komputer stacjonarny, laptop, smartfon, tablet itp. Dopuszcza się używanie urządzeń prywatnych, z zachowaniem wymagań w zakresie bezpieczeństwa określonych w niniejszych zasadach.
2. W przypadku udostępnienia przez Uczelnię modemu Internetowego lub telefonu służbowego z dostępem do Internetu, który może pełnić funkcję HotSpot, to osoba świadcząca pracę zdalną zobowiązana jest korzystać w pierwszej kolejności z tych urządzeń. Przekazany sprzęt należy wykorzystywać jedynie do celów służbowych.
3. Urządzenie służbowe jest przekazywane na podstawie protokołu zdawczo-odbiorczego. Osoba otrzymująca sprzęt jest za niego materialnie odpowiedzialna szczególnie w przypadku uszkodzenia lub zniszczenia przekazanego sprzętu.
4. Sekcja ds. Informatyzacji odnotowuje, które urządzenia są wykorzystywane do pracy zdalnej. W szczególnych przypadkach jeżeli jest to niezbędne, przeprowadza ich przegląd.
5. W przypadku, gdy przegląd stacjonarny jest niemożliwy, na żądanie pracownika Sekcji ds. Informatyzacji można dokonać zdalnego przeglądu, z wykorzystaniem zaproponowanego przez Sekcję narzędzia. Osoba świadcząca pracę zdalną, zobowiązana jest do udostępnienia sprzętu. W przypadku odmowy osoba jest zobowiązana do wykonywania pracy zdalnej w siedzibie Uczelni.

§ 4.

Wymogi bezpieczeństwa dotyczące sprzętu

1. Wymagania w zakresie bezpieczeństwa:
 - 1) urządzenie posiada legalne i aktualne oprogramowanie;
 - 2) zostały włączone automatyczne aktualizacje i zapora systemowa;

- 3) zainstalowany jest i działa w tle program antywirusowy;
- 4) zalogowanie do systemu operacyjnego wymaga uwierzytelnienia, np. poprzez indywidualny login i hasło użytkownika, kod PIN, token;
- 5) wyłączono autouzupełnianie i zapamiętywanie haseł w przeglądarce internetowej;
- 6) zainstalowano program umożliwiający zaszyfrowanie i odszyfrowanie danych (np. 7-zip);
- 7) ustawione zostało automatyczne blokowanie urządzenia po dłuższym braku aktywności;
- 8) jeżeli urządzenie daje taką możliwość, praca może być wykonywana na koncie z ograniczonymi uprawnieniami;
2. Uczelnia może dodatkowo wymagać, aby urządzenie wykorzystywane do pracy zdalnej zawierało inne zabezpieczenia, jak:
 - 1) zaszyfrowany dysk;
 - 2) wyłączone porty pamięci zewnętrznych;
 - 3) oprogramowanie służące monitorowaniu wykonywania pracy, wykorzystywane było zgodnie z wymaganiami przepisów prawa pracy;
3. Zabronione jest udostępnianie urządzeń wykorzystywanych do realizowania pracy zdalnej innym osobom, np. domownikom. Jeśli do pracy zdalnej wykorzystywane jest urządzenie prywatne, z którego korzystają inne osoby, należy założyć osobne konto w systemie operacyjnym, zabezpieczone hasłem.

§ 5.

Zabezpieczanie przekazywanych informacji

1. Do pracy zdalnej powinny być wykorzystywane wyłącznie programy i systemy udostępnione przez Uczelnię.
2. W przypadku, gdy 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 podlegają 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-em,
6. Hasło powinno być silne i zawierać minimum 6 znaków w tym duża litera, cyfra oraz znak specjalny.
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. Przy wysłaniu wiadomości należy dochować należytej staranności, w szczególności sprawdzić, 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. Szczegółowe zasady korzystania z poczty e-mail określa Polityka Ochrony Danych Osobowych Państwowej Wyższej Szkoły Zawodowej im. Witelona w Legnicy.
12. Masowe wysyłki wiadomości e-mail należy realizować poprzez specjalne oprogramowanie udostępnione w tym celu przez Uczelnię.

§ 6.

Zasady korzystania z dokumentów w formie papierowej

1. Zabronione jest zabieranie w miejsce świadczenia pracy zdalnej oryginałów dokumentów. Jeżeli do pracy zdalnej niezbędny jest dostęp do dokumentów papierowych, należy zgłosić prośbę o możliwość ich skopiowania oraz zabrania poza siedzibę Uczelni na czas wykonywania pracy zdalnej, od osoby wymienionej w § 1 ust. 2.
2. Po uzyskaniu zgody i skopiowaniu dokumentów należy sporządzić ich zestawienie, zawierające informacje jakie dokumenty, w jakiej liczbie zostały skopiowane. Zestawienie jest przekazywane odpowiednio osobie wskazanej w § 1 ust. 2
3. Po zakończeniu okresu pracy zdalnej, wszystkie dokumenty należy zwrócić.

§ 7.

Działania niedozwolone

Zakazane jest:

- 1) pozostawianie niezablokowanego komputera, smartfona, tableta bez nadzoru;
- 2) udostępnianie osobom postronnym danych służących do uwierzytelnienia do systemów i/lub usług;
- 3) przekazywanie informacji chronionych, w szczególności danych osobowych bez zabezpieczenia hasłem,

w szczególności w treści wiadomości e-mail oraz 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 Uczelnię;
- 5) udostępnianie służbowego sprzętu lub sprzętu wykorzystywanego do realizowania zadań służbowych innym osobom;
- 6) dzielenie się informacjami poufnymi z innymi osobami, w szczególności domownikami;
- 7) samodzielnego niszczenie dokumentów służbowych w domu;
- 8) logowanie się na konto innego użytkownika;
- 9) kserowanie i zabieranie do miejsca świadczenia pracy, dokumentów bez pisemnej lub elektronicznej zgody osoby wskazanej w §1 ust. 2;
- 10) pozostawienie kserokopii służbowych dokumentów w miejscu świadczenia pracy zdalnej, po zakończeniu świadczenia takiej pracy,
- 11) podejmowanie pracy zdalnej w miejscach publicznych typu: kawiarnie, restauracje, galerie handlowe,

§ 8.

Postanowienia końcowe

1. Problemy w działaniu udostępnionego sprzętu lub oprogramowania należy niezwłocznie zgłaszać do Sekcji ds. Informatyzacji.
2. W przypadku zgubienia lub kradzieży sprzętu, dokumentów lub innych nośników informacji, należy niezwłocznie, w tym samym dniu zgłosić zdarzenie pracodawcy, Sekcji ds. Informatyzacji, a także Inspektorowi Ochrony Danych Osobowych.
3. Postanowienia niniejszych zasad bezpieczeństwa pracy zdalnej mają zastosowanie również do osób prowadzących zajęcia na innej podstawie niż umowa o pracę.
4. W sprawach nieuregulowanych zastosowanie mają wewnętrzne procedury obowiązujące w Uczelni oraz przepisy prawa powszechnie obowiązującego.

