

REGULAMIN PRACY ZDALNEJ
w
Samorządowym Kolegium Odwoławczym w Poznaniu
z dnia 03.08.2023r.

obowiązuje od 18 sierpnia 2023r.

I. CEL REGULAMINU

1. Regulamin pracy zdalnej w Samorządowym Kolegium Odwoławczym w Poznaniu, zwany dalej „Regulaminem”, określa zasady bezpiecznego przetwarzania informacji w formie nieautomatyzowanej – na dokumentach papierowych oraz w formie zautomatyzowanej – w systemach teleinformatycznych, w ramach funkcjonującej pracy zdalnej.
2. Pracownicy Samorządowego Kolegium Odwoławczego w Poznaniu, zwanego dalej „kolegium”, są zobowiązani do przestrzegania Regulaminu oraz do stosowania odpowiednio regulacji wewnętrznych obowiązujących w kolegium, w szczególności „Polityki bezpieczeństwa danych osobowych i bezpieczeństwa teleinformatycznego w Samorządowym Kolegium Odwoławczym w Poznaniu” oraz procedur i instrukcji dotyczących korzystania z narzędzi informatycznych i bezpiecznej pracy z danymi.
3. Odrębne zasady obowiązują podmioty zewnętrzne mające dostęp do danych kolegium, na przykład świadczące wsparcie i serwis techniczno-informatyczny, bądź realizujące usługi na dokumentach papierowych poza siedzibą urzędu.

II. ZASADY PRACY ZDALNEJ

1. Wszelkie informacje służbowe, w szczególności dane osobowe i informacje prawnie chronione, łącznie zwane dalej „danymi” lub „informacjami”, przetwarzane poza siedzibą kolegium, powinny być chronione przed przypadkowym lub niezgodnym z prawem zniszczeniem, utraceniem, zmodyfikowaniem, nieuprawnionym ujawnieniem lub nieuprawnionym dostępem do nich.
2. Pracownik odpowiada za zapewnienie właściwych warunków umożliwiających mu skuteczną pracę zdalną z zachowaniem właściwego poziomu bezpieczeństwa informacji, w tym ochrony danych osobowych.
3. Praca zdalna powinna być realizowana z wykorzystaniem sprzętu służbowego typu: pendrive, laptop, notebook, smartfon, tablet lub innych narzędzi niezbędnych do wykonywania pracy, z zastrzeżeniem pkt 8., natomiast stosowanie sprzętu prywatnego jest dozwolone pod warunkiem spełnienia łącznie warunków od 1) do 5):

- 1) pracownik nie posiada sprawnego służbowego sprzętu typu laptop lub notebook;
 - 2) prywatny sprzęt komputerowy należy do danego pracownika a konto którym się loguje na tym sprzęcie jest dostępne wyłącznie dla niego i jest zabezpieczone bezpiecznym hasłem a sprzęt posiada aktualne oprogramowanie, w tym antywirusowe.
 - 3) komputer prywatny nie posiada konta z dostępem publicznym typu gość, innego konta bez zabezpieczenia bezpiecznym hasłem lub z dostępem bez hasła;
 - 4) żadne przetwarzane na rzecz kolegium pliki danych nie są przechowywane na prywatnym sprzęcie komputerowym a jedynie na odpowiednio zabezpieczonym służbowym pendrive, dysku zewnętrznym lub innym służbowym narzędziu do przechowywania danych, które nie jest pozostawiane bez nadzoru w stanie podłączonym do prywatnego sprzętu komputerowego;
 - 5) każdorazowo po zakończeniu pracy zdalnej na prywatnym sprzęcie komputerowym a przed opuszczeniem tego stanowiska pracy, w przypadku stwierdzenia powstania tymczasowych plików roboczych, muszą one zostać każdorazowo usunięte oraz obligatoryjnie należy opróżnić kosz systemowy.
4. Komunikacja telefoniczna z pracownikiem w trakcie pracy zdalnej odbywa się z wykorzystaniem służbowego numeru komórkowego na służbowy lub prywatny telefon komórkowy.
 5. Do pracy zdalnej należy korzystać z zabezpieczonej silnym hasłem sieci domowej lub sieci komórkowej. Zabronione jest łączenie się za pośrednictwem darmowych, ogólnodostępnych lub nieznanych hot spotów Wi-Fi.
 6. Służbowy przenośny sprzęt komputerowy jest wyposażony w mechanizmy zabezpieczające związane z dostępem do danych.
 7. Administrator może przekazać pracownikowi odpowiednio przygotowany służbowy przenośny sprzęt komputerowy oraz niezbędne parametry uwierzytelniające, wraz z informacją o sposobie ich użycia.
8. Zabronione jest:
 - 1) samodzielne ingerowanie w konfigurację, w szczególności konfigurację VPN na służbowym przenośnym sprzęcie komputerowym;
 - 2) udostępnianie parametrów logowania do elektronicznego systemu obiegu dokumentów w celu ich wykorzystywania przez innego pracownika kolegium lub osoby trzecie;
 - 3) udostępnianie służbowego przenośnego sprzętu komputerowego osobom trzecim, w tym na przykład przekazywanie do zewnętrznych serwisów naprawczych.

9. Zablokowanie dostępu pracownika do zasobów kolegium przy wykorzystaniu (usunięcie lub blokada konta użytkownika) odbywa się po otrzymaniu przez administratora zgłoszenia od bezpośredniego przełożonego. W nagłych przypadkach zgłoszenie może być poprzedzone informacją telefoniczną. Administrator może również podjąć natychmiastową decyzję blokady konta po stwierdzeniu nieuprawnionego dostępu, wystąpieniu incydentu bezpieczeństwa teleinformatycznego lub kradzieży służbowego przenośnego sprzętu komputerowego.
10. Każdorazowo o założeniu, blokadzie lub usunięciu konta dostępu zdalnego administrator informuje Inspektora Ochrony Danych w kolegium.

III. BEZPIECZEŃSTWO FIZYCZNE

1. Miejsce wykonywania pracy zdalnej, w którym pracownik przetwarza dane, stanowi obszar chroniony, który podlega obowiązkowi zastosowania przez pracownika adekwatnych zabezpieczeń tych danych.
2. Zabezpieczenia, o których mowa powyżej, mogą polegać w szczególności na:
 - 1) wydzieleniu miejsca pracy;
 - 2) wydzieleniu miejsca przechowywania służbowego przenośnego sprzętu komputerowego oraz dokumentów służbowych;
 - 3) zapewnieniu, aby osoby nieuprawnione nie miały wglądu w wykonywaną pracę na przykład poprzez odpowiednie ustawienie ekranu komputera;
 - 4) uniemożliwienie wglądu w dokumenty papierowe;
 - 5) prowadzenie służbowych rozmów telefonicznych w sposób gwarantujący ich poufność.
3. Dokumenty papierowe oraz sprzęt służbowy należy transportować w sposób zapobiegający ich kradzieży, zagubieniu, zniszczeniu lub utracie. Zabronione jest pozostawianie dokumentów oraz sprzętu służbowego bez nadzoru w miejscach publicznych, samochodach, publicznych środkach transportu. Do transportu można użyć nieprzejrzystych teczek, zaklejonych kopert itp.

IV. ZABEZPIECZANIE DANYCH PAPIEROWYCH

1. Należy unikać przetwarzania służbowych dokumentów papierowych podczas pracy zdalnej, z uwagi na wysokie ryzyko ich utraty lub zniszczenia. W pierwszej kolejności pracownik w trakcie pracy zdalnej powinien posługiwać się niezbędnymi do realizacji zadań dokumentami elektronicznymi.
2. Jeżeli jednak zachodzi konieczność pracy na dokumentach papierowych, rekomendowane są rozwiązania w postaci: ewidencjonowania dokumentów

przetwarzanych poza kolegium na pracy zdalnej, posługiwanie się kopiami dokumentów papierowych (pozostawianie oryginałów w kolegium) itp.

3. Pracownik, po zakończonym dniu pracy, powinien dbać o zachowanie zasady czystego biurka i bezpieczeństwo dokumentów zawierających dane osobowe.
4. Wszelkie wydruki, kopie dokumentów należy, po zakończeniu pracy zdalnej, dostarczyć do siedziby kolegium i w razie potrzeby te zbędne zniszczyć w niszczarkach w kolegium (zasada czystego kosza na śmieci).

V. ZABEZPIECZANIE DANYCH W SYSTEMACH TELEINFORMATYCZNYCH

A. Bezpieczeństwo teleinformatyczne

1. W trakcie pracy zdalnej należy korzystać ze zdalnego dostępu z elektronicznym systemem obiegu dokumentów obowiązującym w kolegium przy użyciu bezpiecznego łącza internetowego a przy dostępności SSL VPN wyłącznie z tego łącza.
2. Praca w systemach informatycznych, aplikacjach, na dyskach domenowych lub chmurowych kolegium powinna odbywać się zgodnie z obowiązującymi w tym zakresie wewnętrznymi regulacjami, to jest „Polityką bezpieczeństwa danych osobowych i bezpieczeństwa teleinformatycznego w Samorządowym Kolegium Odwoławczym w Poznaniu” oraz procedurami i instrukcjami, w szczególności:
 - 1) logowanie do elektronicznego systemu obiegu dokumentów obowiązującym w kolegium w trakcie pracy zdalnej, powinno odbywać się za pomocą indywidualnego loginu i hasła;
 - 2) hasła i parametry uwierzytelniania do elektronicznego systemu obiegu dokumentów obowiązującym w kolegium nie powinny być przechowywane w formie jawnej, ujawniane w sposób celowy lub przypadkowy i powinny być znane wyłącznie ich użytkownikowi. W przypadku podejrzenia, że parametry logowania zostały ujawnione, należy natychmiast zgłosić ten fakt administratorowi w celu nadania nowych parametrów dostępowych;
 - 3) w przypadku chwilowego odejścia, opuszczenia stanowiska pracy należy stosować „zasadę czystego ekranu, to jest zablokować dostęp do komputera np. skrótem klawiszowym: Windows+L, aby powrót do pracy był możliwy wyłącznie po ponownym uwierzytelnieniu za pomocą hasła;
 - 4) po zakończeniu pracy należy wylogować się z elektronicznego systemu obiegu dokumentów obowiązującym w kolegium, rozłączyć nawiązane połączenie internetowe, usunąć tymczasowe pliki internetowe używanej do pracy przeglądarki

internetowej a następnie prawidłowo zamknąć służbowy lub prywatny przenośny sprzęt komputerowy;

- 5) w celu zapobiegania utracie przetwarzanych danych należy cyklicznie wykonywać archiwizację danych swojego służbowego komputera.
3. Każdy pracownik jest zobowiązany do monitorowania aktualności oprogramowania antywirusowego zainstalowanego na służbowym lub prywatnym przenośnym lub stacjonarnym sprzęcie komputerowym.
4. Do przenoszenia lub wzajemnego udostępniania danych należy wykorzystywać jedynie narzędzia i metody autoryzowane, zalecane przez Inspektora Danych Osobowych.
5. Wydruki dokumentów powinny być wykonywane wyłącznie w siedzibie kolegium, z zachowaniem zasad bezpieczeństwa w trakcie wydruku sieciowego (niepozostawianie wydruków bez nadzoru).
6. Zabronione jest:
 - 1) korzystanie z prywatnych usług chmurowych dla celów związanych z pracą wykonywaną na rzecz kolegium na przykład Google;
 - 2) drukowanie dokumentów w ogólnodostępnych punktach ksero.
7. Pomoc techniczna, naprawy, aktualizacja oprogramowania na służbowym przenośnym sprzęcie komputerowym mogą odbywać się wyłącznie za pośrednictwem podmiotu świadczącego usługi informatyczne na rzecz kolegium i w porozumieniu z informatykiem, na zasadach ogólnie obowiązujących. Zabronione jest samodzielne ingerowanie w konfigurację sprzętu. Zakaz nie dotyczy wymiany elementów zewnętrznych typu myszka, klawiatura, które ulegają naturalnemu zużyciu oraz akceptacji automatycznych aktualizacji sygnalizowanych przez oprogramowanie komputera.
8. Wsparcie techniczne może odbywać się w trybie zdalnym lub – jeśli zachodzi taka konieczność – niezbędne może być osobiste dostarczenie służbowego przenośnego sprzętu komputerowego do siedziby kolegium, po wcześniejszym umówieniu terminu z informatykiem kolegium.
9. W innych celach, związanych z użytkowaniem służbowego przenośnego sprzętu komputerowego, należy stosować wewnętrzne regulacje obowiązujące w kolegium, w szczególności w zakresie odpowiedzialności za powierzony sprzęt i dbałości o niego, podlegania cyklicznej inwentaryzacji.

B. Internet i poczta elektroniczna

1. Podstawowym kanałem komunikacji elektronicznej w trakcie wykonywania pracy zdalnej jest poczta elektroniczna kolegium pod adresem <https://poczta.wokiss.pl/>

2. Zabronione jest korzystanie z prywatnej poczty elektronicznej do przesyłania danych służbowych.
3. Dane osobowe mogą być przesyłane „na zewnątrz” wyłącznie po uprzednim ich zabezpieczeniu na przykład poprzez stosowanie spakowanych załączników do wiadomości e-mailowych zabezpieczonych hasłem przy użyciu programu Zip, 7-zip lub OpenPGP (przekazanie hasła inną drogą komunikacji na przykład telefonicznie lub sms-em) lub szyfrowanie całych wiadomości e-mail przy użyciu narzędzia OpenPGP.
4. Każda wiadomość e-mail powinna być wysyłana „na zewnątrz” z należytą starannością, polegającą w szczególności na sprawdzeniu, czy jest kierowana do właściwego odbiorcy.
5. W przypadku wysyłania wiadomości e-mail do odbiorców, którzy nie znają się wzajemnie, lub ich adresy e-mail są adresami prywatnymi, lub masowej wysyłki wiadomości e-mail, należy adresy e-mail wpisać w pole „Ukryta kopia” (UDW).
6. W trakcie wykorzystywania poczty elektronicznej należy zachować szczególną ostrożność, w szczególności:
 - 1) uważnie czytać treść e-maili;
 - 2) nie podawać danych osobowych, identyfikatorów lub haseł w odpowiedzi na maile;
 - 3) nie otwierać linków lub załączników niewiadomego pochodzenia;
 - 4) nie przysyłać dużych załączników, ponieważ w ten sposób ogranicza się pojemność skrzynki pocztowej;
 - 5) w tytule poczty nie wpisywać treści wskazujących, że wiadomość zawiera dane osobowe;
 - 6) zachować czujność w przypadku otrzymania informacji związanych w jakikolwiek sposób z kwestiami finansowymi;
 - 7) stosować się do wskazówek i informacji dotyczących zagrożeń, przekazywanych z kolegium.
7. Pracownik ponosi pełną odpowiedzialność za korzystanie na służbowym przenośnym sprzęcie komputerowym z Internetu i poczty elektronicznej w sposób, który mógłby spowodować szkody lub naruszyć ochronę przetwarzanych danych.

VI. INCYDENTY BEZPIECZEŃSTWA

W przypadku wystąpienia incydentu bezpieczeństwa teleinformatycznego, w tym naruszenia ochrony danych osobowych, należy postępować zgodnie z „Instrukcją postępowania z incydentami”, stanowiącą załącznik do „Polityki bezpieczeństwa danych osobowych i bezpieczeństwa teleinformatycznego w Samorządowym Kolegium Odwoławczym w Poznaniu”.

VII. POSTANOWIENIA KOŃCOWE

- 1.** Przy przetwarzaniu wszelkich informacji, a w szczególności danych osobowych należy kierować się przede wszystkim zasadami dotyczącymi przetwarzania danych osobowych, zawartymi w art. 5 RODO, tj.:
 - 1)** zasadą zgodności z prawem, rzetelności i przejrzystości;
 - 2)** zasadą ograniczenia celu;
 - 3)** zasadą minimalizacji danych;
 - 4)** zasadą prawidłowości;
 - 5)** zasadą ograniczenia przechowywania;
 - 6)** zasadą integralności i poufności;
 - 7)** zasadą rozliczalności.
- 2.** W ramach uprawnienia pracodawcy do kontroli pracy zdalnej, może ona dotyczyć przestrzegania wymogów w zakresie bezpieczeństwa i ochrony informacji, w tym przestrzegania Regulaminu.
- 3.** Każdy pracownik przed rozpoczęciem świadczenia pracy zdalnej jest zobowiązany do złożenia oświadczenia, którego wzór jest określony w załączniku do Regulaminu, z zastrzeżeniem ust. 4.
- 4.** W przypadku świadczenia okazjonalnej pracy zdalnej, oświadczenie należy złożyć przed pierwszym dniem pracy zdalnej w danym roku kalendarzowym.

OŚWIADCZENIE

Ja, niżej podpisana/y oświadczam, że:

- 1) w związku z pracą zdalną zapewniam środki techniczne i organizacyjne umożliwiające bezpieczne przetwarzanie informacji, w tym danych osobowych, w zgodzie z obowiązującymi przepisami prawa i wewnętrznymi regulacjami w tym zakresie;
- 2) zapoznałam/em się z:
 - a) regulaminem pracy zdalnej w Samorządowym Kolegium Odwoławczym w Poznaniu, zatwierdzonym dnia 3 sierpnia 2023 r.,
 - b) „Polityką bezpieczeństwa danych osobowych i bezpieczeństwa teleinformatycznego w Samorządowym Kolegium Odwoławczym w Poznaniu,
 - c) ustawą z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz. U. z 2019 r. poz. 1781),
 - d) rozporządzeniem Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz. Urz. UE L 119 z 4.05.2016, str. 1, z późn. zm.)

i zobowiązuje się do ich przestrzegania.

Jednocześnie zobowiązuje się do nieujawniania w jakiegokolwiek postaci treści pozyskanych informacji oraz sposobów ich zabezpieczania. Obowiązek zachowania tajemnicy jest nieograniczony w czasie i nie ustaje z chwilą ustania zatrudnienia.

.....
data i czytelny podpis