Załącznik nr 1
do zarządzenia Rektora nr 23/2023
z dnia 3 lipca. 2023 r.

PROCEDURA OCHRONY DANYCH OSOBOWYCH PRZY PRACY ZDALNEJ

1. Każdy pracownik Państwowej Wyższej Szkoły Zawodowej w Głogowie, w tym również wykonujący pracę w trybie pracy zdalnej, jest zobowiązany do przestrzegania postanowień Polityki Bezpieczeństwa Informacji obowiązującej w Uczelni, niezależnie od miejsca wykonywania pracy.
2. Niniejsze Procedury określają zasady przetwarzania danych osobowych, których administratorem jest Państwowa Wyższa Szkoła Zawodowa w Głogowie (dalej jako: „Pracodawca" lub „PWSZ"), podczas wykonywania pracy zdalnej.
3. Każdy pracownik wykonujący pracę zdalną ma obowiązek zapoznania się z niniejszymi procedurami i podpisania oświadczenia stanowiącego załącznik nr 1.

Organizacja miejsca pracy

1. Pracownik ma obowiązek organizacji miejsca wykonywania pracy zdalnej w sposób zapewniający ochronę danych osobowych.
2. Pracę należy wykonywać w osobnym pokoju lub wyznaczonym do tego celu miejscu np. przez faktyczne wydzielenie stanowiska pracy, osobne biurko, miejsce przeznaczone do przechowywania dokumentów lub innych nośników danych.
3. W przypadku chwilowego opuszczania pomieszczenia bądź stanowiska pracy, należy upewnić się, że do wykorzystywanych w trakcie pracy informacji nie będą miały dostępu osoby postronne, w tym domownicy. Dostęp do komputera musi być zablokowany a dokumenty papierowe zabezpieczone, np. poprzez umieszczenie ich w zamykanych szafkach.
4. Jeśli miejsce pracy jest współdzielone z innymi domownikami, należy zapewnić, aby domownicy nie mieli wglądu w wykonywaną pracę, w szczególności poprzez właściwe ustawienie ekranu komputera, pracę z dokumentami w sposób uniemożliwiający wgląd.
5. Zabronione jest prowadzenie rozmów służbowych (telefonicznych, wideokonferencji) lub służbowej korespondencji w miejscach, które nie gwarantują zapewnienia poufności (np. środki komunikacji publicznej, inne miejsca dostępne publicznie, winda, balkon, itp.).
6. Kończąc korzystanie ze służbowego telefonu należy upewnić się, że urządzenie zostało zablokowane.
7. Po zakończeniu pracy należy wyłączyć urządzenia elektroniczne i umieścić wszystkie elektroniczne i papierowe nośniki informacji (dokumenty) w szafkach, a jeśli to możliwe - zamykanych na klucz. Obowiązuje zasada czystego biurka.
8. Podejmowanie pracy zdalnej w miejscach publicznych (galerie handlowe, kawiarnie, restauracje itp.), gdzie osoby postronne mogłyby usłyszeć fragmenty rozmów lub mieć wgląd w wykonywaną pracę, jest zabronione.

Praca z dokumentacją w formie papierowej

1. Pracownik ma obowiązek zapewnienia bezpieczeństwa dokumentacji przed wglądem osób nieupoważnionych (np. pozostawianie ich w sposób, który umożliwi innym zapoznanie się z treścią dokumentów) oraz przed zniszczeniem, uszkodzeniem, zabraniem przez osoby nieupoważnione. Dotyczy to także wszelkich kopii dokumentów.

2. Wszystkie wydruki, skanowane lub kopiowane dokumenty powinny być niezwłocznie usuwane z urządzeń, w celu uniemożliwienia zapoznania się z nimi osobom postronnym.
3. Po zakończonej pracy dokumenty należy przechowywać w bezpiecznym miejscu jak np. zamykane szafki, aktówki, teczki do przechowywania dokumentów, odkładane w miejsce poza zasięgiem domowników, w szczególności dzieci.
4. Obowiązuje ogólny zakaz wynoszenia dokumentów lub ich kopii poza teren Uczelni.
5. W wyjątkowych przypadkach, gdy do pracy zdalnej niezbędny jest dostęp do dokumentów w formie papierowej, pracownik zgłasza do kierownika komórki organizacyjnej/kierownika jednostki prośbę o możliwość ich skopiowania oraz wyniesienia poza teren zakładu pracy, na czas wykonywania pracy zdalnej. Po otrzymaniu zgody na piśmie (także w formie służbowej wiadomości e-mail), pracownik może sporządzić kopie niezbędnych dokumentów. Kopie należy sporządzić korzystając ze sprzętu na terenie Uczelni.
6. Zabronione jest zabieranie poza teren zakładu pracy oryginałów dokumentów.
7. Podczas przewożenia dokumentów do miejsca wykonywania pracy zdalnej, należy zachować szczególną ostrożność i zabezpieczyć dokumenty przed ich zagubieniem, zniszczeniem, uszkodzeniem, zabraniem przez osoby nieupoważnione.
8. Niedozwolone jest wykonywanie pracy z dokumentami w miejscu publicznym (kawiarnia, restauracja, galeria handlowa, itp.). Zabronione jest także korzystanie z ogólnodostępnych punktów ksero do powielania dokumentów zawierających dane służbowe, a w szczególności dane osobowe.
9. Po zakończeniu pracy zdalnej, wykonane kopie dokumentów należy przekazać do siedziby Pracodawcy celem ich zniszczenia w odpowiednich urządzeniach.
10. Zaleca się, aby praca zdalna była wykonywana wyłącznie w formie elektronicznej, tj. bez korzystania z wydruków roboczych dokumentów. W przypadku konieczności wykonania wydruku zawierającego dane osobowe, po zakończeniu pracy z dokumentem lub jego kopią, która nie jest dłużej potrzebna bądź nie wymaga archiwizowania, dokument należy niezwłocznie zniszczyć z wykorzystaniem niszczarki bądź przekazać Pracodawcy.

Zasady bezpieczeństwa pracy zdalnej

1. Wszyscy pracownicy Uczelni: pracownicy administracyjni a także wykładowcy zobowiązani są do ochrony danych osobowych. Szczególnie podczas pracy zdalnej, przenoszenia oraz udostępniania plików, które te dane zawierają.
2. Przenosząc, lub przechowując takie dane na dyskach zewnętrznych lub pendrive'ach, konieczne jest ich zabezpieczenie przed dostaniem się w niepowołane ręce. Ta sama sytuacja dotyczy załączników dodawanych do wiadomości e-mail zawierających w/w treści.
3. We wszystkich tych przypadkach należy stosować się do „Instrukcji zabezpieczania danych udostępnianych i przenoszonych na nośnikach zewnętrznych" obowiązującej w Uczelni.

Urządzenia stanowiące własność Pracodawcy (służbowe)

1. Praca zdalna powinna być realizowana z wykorzystaniem urządzeń służbowych, tzn. otrzymanych od Pracodawcy: laptopa, komputera stacjonarnego, telefonu, tabletu, itp.
2. W przypadku narzędzi należących do Pracodawcy, do pracy zdalnej dopuszczone są wyłącznie komputery przygotowane przez Sekcję IT.
3. Urządzenie służbowe jest udostępniane pracownikowi na potrzeby pracy zdalnej po spełnieniu warunków określonych w Instrukcji zarządzania systemem informatycznym,

stanowiącej załącznik nr 1 do zarządzenia nr 69/2020 Rektora Państwowej Wyższej Szkoły Zawodowej w Głogowie z dnia 9 września 2020 roku (w tym podpisaniu wskazanego w Instrukcji oświadczenia).

4. Niedozwolone jest udostępnianie służbowych urządzeń wykorzystywanych do pracy zdalnej innym osobom, w tym domownikom.
5. Niedozwolone jest korzystanie z urządzeń służbowych do celów niezwiązanych z wykonywaniem obowiązków na danym stanowisku pracy.
6. Niedozwolone jest kopiowanie informacji służbowych na prywatne urządzenia.
7. Praca na komputerze wykonywana jest wyłącznie na koncie z ograniczonymi uprawnieniami, tj. koncie użytkownika.
8. Zalogowanie do systemu operacyjnego urządzenia wymaga uwierzytelnienia poprzez indywidualny login i hasło. Obowiązkiem pracownika jest zapewnienie poufności haseł dostępowych.
9. Niedozwolone jest korzystanie z jakiegokolwiek oprogramowania komputerowego innego niż oprogramowanie dostarczone przez Sekcję IT, w szczególności dokonywanie instalacji takiego oprogramowania na urządzeniach.
10. Pracownik może korzystać z zewnętrznych nośników danych tylko po uprzednim sprawdzeniu zawartości nośnika oprogramowaniem antywirusowym.
11. Podczas transportu urządzenia pracownik jest zobowiązany do zachowania szczególnej ostrożności, w szczególności do zabezpieczenia go przed kradzieżą i dostępem osób nieuprawnionych.

Urządzenia stanowiące własność pracownika (prywatne)

1. Pracownik może wykonywać pracę zdalną za pomocą narzędzi pracy niezapewnionych przez Pracodawcę (urządzeń prywatnych). W tym przypadku należy spełnić warunki, o których mowa w Instrukcji zarządzania systemem informatycznym, stanowiącej załącznik nr 1 do zarządzenia nr 69/2020 Rektora Państwowej Wyższej Szkoły Zawodowej w Głogowie z dnia 9 września 2020 roku, część IV – Procedura nadawania uprawnień do korzystania z prywatnego sprzętu IT (w tym podpisaniu wskazanego w Instrukcji oświadczenia).
2. W przypadku, gdy z urządzeń prywatnych wykorzystywanych do pracy zdalnej korzystają także inny domownicy, niezbędne jest wydzielenia osobnego konta użytkownika w systemie (pracownik wykonuje obowiązki służbowe wyłącznie w przeznaczonym do tego celu koncie użytkownika).
3. Zalogowanie do systemu operacyjnego lub konta użytkownika, o którym mowa powyżej wymaga uwierzytelnienia poprzez indywidualny login i hasło. Obowiązkiem pracownika jest zapewnienie poufności haseł dostępowych.
4. Pracownik może korzystać z zewnętrznych nośników danych tylko po uprzednim sprawdzeniu zawartości nośnika oprogramowaniem antywirusowym.
5. Pracownik wykonujący pracę zdalną za pomocą urządzeń prywatnych będzie miał dostęp wyłącznie do usług udostępnianych przez Pracodawcę w internecie.
6. Minimalne wymagania w zakresie bezpieczeństwa:
    a) urządzenie posiada legalne i aktualne oprogramowanie,
    b) urządzenie posiada włączone automatyczne aktualizacje oprogramowania,
    c) urządzenie posiada włączoną zaporę systemową,
    d) na urządzeniu został zainstalowany i działa w tle program antywirusowy,

e) zalogowanie do systemu operacyjnego lub konta użytkownika wymaga uwierzytelnienia 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 zastosowane automatyczne blokowanie urządzenia po dłuższym braku aktywności.

Korzystanie z internetu

1. W przypadku korzystania z domowej sieci WiFi, należy upewnić się, że została ona skonfigurowana w sposób minimalizujący ryzyko naruszenia poufności informacji, w szczególności:

   a) korzystanie z internetu wymaga uwierzytelnienia poprzez hasło,

   b) hasło dostępowe składa się z co najmniej 8 znaków, w tym z dużych i małych liter oraz cyfr i znaków specjalnych,

   c) dostęp do panelu administracyjnego routera jest możliwy wyłącznie z urządzeń znajdujących się w sieci domowej,

   d) jeśli to możliwe, należy zmienić login do panelu administracyjnego routera na własny i zmienić domyślny adres routera na inny.

2. Niedozwolone jest korzystanie z publicznych sieci WiFi o otwartym dostępie (np. w środkach komunikacji publicznej, hotelach, restauracjach, centrach handlowych, itp.) w trakcie wykonywanie pracy zdalnej.

Zabezpieczanie informacji przesyłanych za pomocą poczty elektronicznej (e-mail)

1. Korespondencja e-mail dot. spraw służbowych, prowadzona jest w trakcie wykonywania pracy zdalnej wyłącznie przy pomocy adresu e-mail w domenie Uczelni „pwsz.glogow.pl". Zabronione jest korzystanie z innej, w tym prywatnej poczty e-mail w celach służbowych.
2. Jeżeli informacje służbowe, w szczególności dane osobowe, są przesyłane za pomocą poczty e-mail, powinny zostać udostępnione w załączniku zabezpieczonym hasłem. Hasło powinno być odpowiednio skomplikowane i nieoczywiste.
3. Rekomendowane metody zabezpieczania hasłem/szyfrowania wiadomości zawarte są w „Instrukcji zabezpieczania danych udostępnianych i przenoszonych na nośnikach zewnętrznych".
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 do przesyłanego pliku zostaje przekazane odbiorcy inną drogą komunikacji.
6. Wiadomości powinny być wysyłana z należytą starannością, polegającą w szczególności na sprawdzeniu, czy jest kierowana do odpowiedniego odbiorcy. Za poprawność adresu odbiorcy odpowiedzialny jest nadawca wiadomości.
7. Jeżeli wiadomości wysyłane są do kilku odbiorców nie znających wzajemnie swoich adresów e-mail i/lub korzystających z prywatnych adresów e-mail, adresy te należy wskazać w polu UDW (ukryte do wiadomości). W takim wypadku wiadomość należy zaadresować do siebie, wskazując swój adres e-mail w polu Do.

Sytuacje szczególne

1. Niedopuszczalne jest przetwarzanie w ramach pracy zdalnej informacji niejawnych podlegających ochronie na podstawie ustawy z dnia 5 sierpnia 2010 roku o ochronie informacji niejawnych (t.j. Dz.U. 2023, poz.756).
2. Jakiekolwiek problemy w działaniu urządzeń służbowych lub oprogramowania wykorzystywanych do wykonywania pracy zdalnej, należy niezwłocznie zgłaszać do Sekcji IT.
3. Pracownik zobowiązany jest do informowania bezpośredniego przełożonego o wszelkich problemach i utrudnieniach związanych z zapewnieniem właściwej ochrony danych osobowych.
4. Jeżeli pracownik nie ma możliwości świadczenia pracy zdalnej z zapewnieniem właściwych zabezpieczeń, w szczególności ze względu na siłę wyższą, niezwłocznie zgłasza to bezpośredniemu przełożonemu i postępuje zgodnie z jego instrukcjami.
5. W razie zgubienia lub kradzieży urządzeń, dokumentów lub innych nośników informacji, należy niezwłocznie, w dniu zdarzenia zgłosić je do:
   a) Pracodawcy, e-mail: pawlaczek@pwsz.glogow.pl ,
   b) Sekcja IT, e-mail: administrator@pwsz.glogow.pl
   c) inspektora ochrony danych, e-mail: rudnik@pwsz.glogow.pl
5. Wszelkie podejrzenia naruszenia ochrony danych osobowych, jak np. utrata czy udostępnienie danych osobie nieuprawnionej, itd. należy niezwłocznie zgłaszać bezpośredniemu przełożonemu i inspektorowi ochrony danych. Należy zgłaszać każdą sytuację, która w opinii pracownika odbiega od przyjętej normy i obowiązujących standardów bezpieczeństwa. Ocena ryzyka zdarzenia należy do Pracodawcy.
6. W przypadku wpłynięcia bezpośrednio do pracownika wykonującego pracę zdalną jakiegokolwiek żądania osoby, której dane dotyczą, pracownik przed podjęciem jakichkolwiek działań, konsultuje sposób postępowania, a w szczególności treść udzielanej odpowiedzi z inspektorem ochrony danych.

OPRACOWAŁA: ZATWIERDZIŁA:

Załącznik nr 1
do „Procedury ochrony danych
osobowych przy pracy zdalnej”

.....

imię i nazwisko pracownika

OŚWIADCZENIE

pracownika o zapoznaniu się z procedurą ochrony danych osobowych

Oświadczam, że zapoznałem się z „Procedurą ochrony danych osobowych przy pracy zdalnej” obowiązującą u mojego Pracodawcy, tj. w Państwowej Wyższej Szkole Zawodowej w Głogowie, i zobowiązuję się do jej przestrzegania.

.....

data, miejsce i czytelny podpis pracownika