WÓJT
GMINY NIECHLÓW

Zarządzenie Nr 97/2023

Wójta Gminy Niechlów

z dnia 1 sierpnia 2023 r.

w sprawie: organizowania pracy zdalnej okazjonalnej w Urzędzie Gminy Niechlów.

Na podstawie art. 67 [33] ustawy z dnia 26 czerwca 1974 r. Kodeks pracy (t.j. Dz.U. z 2022, poz. 1510 ze zm.) , art. 33 ust. 3 ustawy z dnia 8 marca 1990 r. o samorządzie gminnym (t.j. Dz.U. z 2023 r. poz. 40) zarządzam, co następuje:

§ 1

1. Pracownicy Urzędu Gminy Niechlów mają prawo do korzystania z pracy zdalnej okazjonalnej w wymiarze 24 dni w roku kalendarzowym. Wymiar dni pracy zdalnej niezależny jest od wymiaru etatu pracownika.

2. Przez pracę zdalną rozumie się pracę wykonywaną w miejscu wskazanym przez pracownika i każdorazowo uzgodnionym z pracodawcą, w tym pod wskazanym adresem zamieszkania pracownika.

3. Wykonywanie pracy zdalnej okazjonalnej jest możliwe, jeśli organizacja pracy i rodzaj wykonywanej pracy na to pozwala.

4. Okres wykonywania pracy zdalnej okazjonalnej jest ewidencjonowany. Niewykorzystane dni limitu pracy zdalnej okazjonalnej nie przechodzą na kolejny rok kalendarzowy.

5. Skorzystanie z pracy zdalnej okazjonalnej wymaga złożenia wniosku pracownika w postaci papierowej lub elektronicznej. Wniosek jest niewiążący dla pracodawcy i wymaga akceptacji przez bezpośredniego przełożonego. Wzór wniosku stanowi **Załącznik Nr 1** do niniejszego zarządzenia.

6. Wniosek o pracę zdalną okazjonalną powinien zostać złożony w formie pisemnej lub papierowej lub elektronicznej co najmniej 1 dzień przed rozpoczęciem dnia pracy.

7. W szczególnie uzasadnionych przypadkach pracodawca może wyrazić zgodę na pracę zdalna okazjonalną na wniosek złożony w tym samym dniu, na który przypada jej rozpoczęcie.

8. We wniosku pracownik określa miejsce wykonywania pracy zdalnej okazjonalnej oraz liczbę dni korzystania z pracy zdalnej okazjonalnej.

9. Pracodawca może wyrazić zgodę na pracę zdalną okazjonalną pod warunkiem, że:

a) rodzaj/charakter pracy pozwala na jej okazjonalne wykonywanie w miejscu wskazanym przez pracownika,

b) pracownik posiada odpowiednie warunki techniczne i lokalowe do wykonywania pracy zdalnej okazjonalnej.

10. Przed złożeniem wniosku pracownik zobowiązany jest do zapoznania się z:

a) procedurą ochrony danych osobowych w związku z wykonywaniem pracy zdalnej okazjonalnej, która stanowi **Załącznik Nr 2,**

b) informacją zawierającą zasady bezpiecznego i higienicznego wykonywania pracy zdalnej okazjonalnej,

c) oceną ryzyka zawodowego na stanowisku pracy zdalnej okazjonalnej.

11. W wyjątkowych sytuacjach bezpośredni przełożony ma prawo wezwać pracownika do biura w dniu, w którym wykonuje on pracę zdalną okazjonalną.

12. Pracodawca zapewnia pracownikowi materiały i narzędzia, w tym urządzenia techniczne niezbędne do wykonywania pracy zdalnej okazjonalnej.

13. W szczególnie uzasadnionych przypadkach pracodawca może zapewnić dostarczenie materiałów i narzędzi, w tym urządzeń technicznych do miejsca wykonywania pracy zdalnej okazjonalnej pracownika.

14. Przekazanie sprzętu komputerowego pracownikowi odbywa się poprzez spisanie protokołu zdawczo-odbiorczego, który stanowi **Załącznik Nr 3** do niniejszego zarządzenia.

§ 2

1. Pracownik wykonuje pracę zdalną okazjonalną w systemie czasu pracy i zgodnie z obowiązującym go rozkładem czasu pracy wynikającym z Regulaminu pracy.

3. Pracownika obowiązują przerwy w pracy zgodnie z przepisami prawa.

4. Pracownik ma prawo do skorzystania z wyjścia prywatnego w związku z koniecznością załatwienia spraw prywatnych w ciągu dnia pracy. Wyjście prywatne jest udzielane na podstawie wniosku wysłanego mailem do bezpośredniego przełożonego i powinno być odpracowane w danym okresie rozliczeniowym.

5. Praca w godzinach nadliczbowych w czasie świadczenia pracy zdalnej może być wykonywana na zasadach określonych w Zarządzeniu Nr 78/2015 Wójta Gminy Niechlów z dnia 30 czerwca 2015 r. w sprawie ustalenia procedury zlecenia i rozliczania godzin nadliczbowych, korzystania z wyjść służbowych i prywatnych oraz ich odpracowywania przez pracowników urzędu Gminy Niechlów.

§ 3

Pracownik jest zobowiązany do:

a) pozostawania w dyspozycji pracodawcy w ustalonych dniach i godzinach pracy oraz przyjmowania bieżących zadań,
b) poświęcania czasu pracy wyłącznie na wykonywanie obowiązków pracowniczych, w tym poleceń bezpośredniego przełożonego, w szczególności na bieżąco sprawdzając korespondencję elektroniczną, odpowiadając na wiadomości, będąc w pełnej dostępności za pomocą telefonu lub adresu mailowego,
c) potwierdzania obecności w pracy w okresie wykonywania pracy zdalnej okazjonalnej w sposób określony z pracodawcą,
d) prowadzenia ewidencji/ raportowanie wykonanych czynności, uwzględniającej opis czynności, a także datę ich wykonania. Wzór ewidencji stanowi **Załącznik Nr 4** do niniejszego zarządzenia.
e) przestrzegania zasad i przepisów dotyczących BHP i ochrony ppoż., w tym zorganizowania stanowiska pracy zdalnej z uwzględnieniem ergonomii,
f) powstrzymania się od wykonywania pracy w przypadku zaistnienia okoliczności powodującej zagrożenie życia i zdrowia a także niezwłocznego poinformowania o tym bezpośredniego przełożonego,
g) przestrzegania procedury ochrony danych osobowych w związku z wykonywanymi zadaniami,
h) zabezpieczenia dostępu do urządzeń, które wykorzystuje w celu pracy zdalnej oraz

posiadanych w związku z pracą zdalną dokumentów, danych i informacji przed wszelkimi osobami postronnymi, w tym wspólnie zamieszkującymi, jak również przed utraceniem, uszkodzeniem lub zniszczeniem urządzeń lub dokumentów,

i) niezwłocznego zawiadomienia bezpośredniego przełożonego w przypadku kradzieży lub zgubienia urządzenia lub zaistnienia incydentu dotyczącego bezpieczeństwa danych osobowych.

j) pracownik zobowiązuje się do używania udostępnionych mu materiałów, narzędzi w tym urządzeń technicznych, oprogramowania wyłącznie do celów służbowych, w sposób zgodny z ich przeznaczeniem.

k) pracownik wykonujący pracę zdalna okazjonalną zobowiązany jest do dbania o powierzone mu mienie pracodawcy, jak również zobowiązany jest aby przechowywać je w miejscu nie dostępnym dla osób trzecich.

§ 4

1. Każdy pracownik wykonujący pracę zdalną okazjonalną jest zobowiązany do zapoznania się z niniejszym zarządzeniem, co powinno nastąpić przed rozpoczęciem wykonywania pracy zdalnej.

2. Za zapoznanie pracowników z niniejszym zarządzeniem odpowiedzialni są bezpośredni przełożeni.

3. Pracownik składa oświadczenie o zapoznaniu się z niniejszym zarządzeniem, które zostanie przekazane do działu kadr w celu umieszczenia go w aktach osobowych. Oświadczenie stanowi **Załącznik Nr 5** do niniejszego zarządzenia.

§ 5

1. Pracodawca ma prawo przeprowadzić kontrolę:

a) wykonywania pracy zdalnej przez pracownika,

b) w zakresie bezpieczeństwa i higieny pracy zdalnej

c) przestrzegania wymogów w zakresie bezpieczeństwa i ochrony informacji, w tym procedur ochrony danych osobowych.

2. Kontrolę przeprowadza pracodawca lub upoważniony pracownik na zasadach ustalonych z pracownikiem w miejscu wykonywania pracy zdalnej w godzinach pracy pracownika.

3. Wykonywanie czynności kontrolnych nie może naruszać prywatności pracownika wykonującego pracę zdalną okazjonalną i innych osób ani utrudniać korzystania z pomieszczeń

domowych w sposób zgodny z ich przeznaczeniem.

4. Kontrola może mieć formę on-line, odbywającej się przez telekonferencję za pośrednictwem telefonu komórkowego lub innej aplikacji.

5. Jeżeli przeprowadzający kontrolę stwierdzi uchybienia w przestrzeganiu przepisów i zasad w zakresie bezpieczeństwa i higieny pracy, lub w nieprzestrzeganiu wymogów w zakresie bezpieczeństwa i ochrony informacji, zobowiązuje pracownika do usunięcia stwierdzonych uchybień we wskazanym terminie.

6. Z przeprowadzonej kontroli nie sporządza się protokołu, jeśli w trakcie podjętych działań nie stwierdzono żadnych nieprawidłowości.

§ 6

1. Pracodawca może wycofać zgodę na wykonywanie pracy zdalnej okazjonalnej w przypadku:
   a) gdy zostanie poinformowany przez pracownika o zmianie warunków lokalowych i technicznych uniemożliwiających wykonywanie pracy zdalnej,
   b) braku usunięcia przez pracownika stwierdzonych uchybień po przeprowadzonej kontroli.
2. W przypadku wycofania przez Pracodawcę zgody na wykonywanie pracy zdalnej okazjonalnej, pracownik rozpoczyna pracę niezwłocznie w dotychczasowym miejscu pracy określonym w umowie o pracę.

§ 7

Pracodawca może odmówić uwzględnienia wniosku pracownika, jeżeli świadczenie pracy okazjonalnej nie jest możliwe ze względu na organizację pracy lub rodzaj pracy wykonywanej przez pracownika. O przyczynie odmowy uwzględnienia wniosku pracodawca informuje pracownika w postaci papierowej lub elektronicznej.

§ 8

Wykonanie zarządzenia powierza się Sekretarzowi Gminy.

§ 9

Zarządzenie wchodzi w życie z dniem podjęcia.

p.o. Wójta Gminy Niechlów
Michał Frąckowiak

Sporządziła: Elżbieta Majchrzak

Załącznik Nr 1
do Zarządzenia Nr 97/2023
Wójta Gminy Niechlów
z dnia 1 sierpnia 2023 r.

.....
(imię i nazwisko pracownika)

.....
(miejscowość, data)

.....
(stanowisko pracy)

Wniosek o pracę zdalną okazjonalną

Na podstawie art. 67^{33} Kodeksu pracy zwracam się o umożliwienie wykonywania pracy zdalnej okazjonalnej w dniu* ..... lub w okresie* od dnia ..... do dnia .....
(wpisać dni robocze pracownika, maksymalnie 24 dni)

Praca zdalna okazjonalna będzie przeze mnie wykonywana pod adresem:
.....
(wpisać miejsce świadczenia pracy w trakcie pracy zdalnej)

Jednocześnie oświadczam, że:

1. Na stanowisku pracy zdalnej w miejscu jej wykonywania są zapewnione bezpieczne i higieniczne warunki pracy.
2. Zapoznałem/am się z przygotowaną przez pracodawcę :
- oceną ryzyka zawodowego,
- informacją zawierającą zasady bezpiecznego i higienicznego wykonywania pracy zdalnej z uwzględnieniem wymagań ergonomii,
- procedurą ochrony danych osobowych w czasie wykonywania pracy zdalnej.
3. Zobowiązuję się do przestrzegania informacji, procedur, wskazówek i wniosków wynikających z dokumentów wskazanych w pkt 2 powyżej,
4. Zasady kontroli wykonywania pracy zdalnej, kontrola w zakresie bezpieczeństwa i higieny pracy są mi znane i potwierdzam wolę ich stosowania w czasie wykonywania pracy zdalnej.

.....
(podpis pracownika)

Potwierdzam/nie potwierdzam*, że organizacja pracy i rodzaj pracy umożliwia wykonywanie pracy zdalnej.
Wyrażam zgodę/ nie wyrażam zgody*

.....
(pieczęć i podpis pracodawcy lub osoby upoważnionej)

*niepotrzebne skreślić

Załącznik Nr 2
do Zarządzenia Nr 97/2023
Wójta Gminy Niechlów
z dnia 1 sierpnia 2023 r.

Procedura ochrony danych osobowych w ramach pracy zdalnej

I. Zakres podmiotowy procedury

1. Procedura określa zasady postępowania z danymi osobowymi w przypadku ich przetwarzania podczas pracy poza siedzibą pracodawcy.
2. Zakresem procedury objęci są pracownicy wykonujący pracę zdalną na podstawie:
   a) art. 67^{19} § 1 Kodeksu pracy (praca zdalna uzgodniona między pracownikiem a pracodawcą),
   b) art. 67^{19} § 3 Kodeksu pracy (obligatoryjna praca wykonywana na polecenie pracodawcy),
   c) art. 67^{19} § 6 Kodeksu pracy (obligatoryjna praca zdalna na wniosek pracownika).

II. Podstawowe pojęcia

1) dane osobowe – wszelkie informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizyczne, np. imię i nazwisko, numer identyfikacyjny (PESEL), adres zamieszkania, adres e-mail,
2) naruszenie ochrony danych osobowych – takie naruszenie bezpieczeństwa, które prowadzi do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych,
3) pracownik wykonujący pracę zdalną – osoba zatrudniona na podstawie przepisów kodeksu pracy, w jeden ze sposobów określonych w art. 67^{19} § 1 Kodeksu pracy (w rozumieniu procedury nie jest pracownikiem wykonującym pracę zdalną osoba zatrudniona na podstawie umów cywilnoprawnych).

III. Obowiązki ogólne

1. Każdy pracownik wykonujący pracę zdalną jest zobowiązany do stosowania obowiązujących w zakładzie pracy wewnętrznych aktów dotyczących ochrony informacji i danych osobowych, a także procedur lub instrukcji dotyczących działania systemów informatycznych obowiązujących u pracodawcy. Wciąg z Polityki Ochrony Danych Osobowych oraz Regulaminu Ochrony Danych Osobowych obowiązujących u Administratora, stanowiący załącznik nr 1 do niniejszej procedury określa w jaki sposób należy przetwarzać dane osobowe poza siedzibą Administratora.
2. Pracownik wykonujący pracę zdalną w sposób wskazany w pkt . I niniejszej procedury wykonuje ją na sprzęcie powierzonym przez Administratora, który został odpowiednio skonfigurowanym i zabezpieczony.
3. Każdy pracownik ma obowiązek uczestniczenia w szkoleniach z zakresu ochrony danych osobowych, na które kieruje go pracodawca.

4. Każdy pracownik ma obowiązek zgłaszania wszelkich podejrzeń naruszeń ochrony danych osobowych. Każdy incydent należy zgłosić na adres agnieszka.siemczonek@iodo@amt24.biz
5. Należy ograniczyć do niezbędnego minimum drukowanie dokumentacji zawierającej dane osobowe, a jeżeli taka konieczność zaistnieje, należy niszczyć wydruki po zakończeniu pracy z nimi.
6. Dokumentację w miejscu wykonywania pracy zdalnej należy zabezpieczyć przed dostępem osób trzecich
7. Nie jest dopuszczalne korzystanie i zapisywanie na własnych nośnikach plików zawierających dane osobowe, których administratorem jest pracodawca, bez jego zgody i bez wcześniejszego zabezpieczenia przez pracodawcę.
8. Nie jest dopuszczalne umożliwianie dostępu do danych, poczty elektronicznej lub systemów informatycznych osobom nieuprawnionym, próbujących uzyskać dostęp drogą telefoniczną lub mailową, podającym się za przedstawicieli serwisu lub konkretnych instytucji, bez ich weryfikacji i potwierdzenia w zakładzie pracy takiego kontaktu.

IV. Obowiązki pracowników korzystających wyłącznie z poczty elektronicznej

Każdy pracownik korzystający z poczty elektronicznej jest zobowiązany do:

1) przechowywania loginu i hasła do poczty elektronicznej w bezpiecznym miejscu, niedostępnym dla osób nieuprawnionych, w tym domowników,
2) korzystania z poczty elektronicznej wyłącznie w celach służbowych,
3) archiwizowania korespondencji służbowej przy użyciu dedykowanych temu celowi narzędzi poczty elektronicznej,
4) nieprzesyłania korespondencji służbowej na jakąkolwiek prywatną skrzynką pocztową.

V. Obowiązki pracowników korzystających z poczty elektronicznej i systemów teleinformatycznych

Każdy pracownik korzystający z poczty elektronicznej i systemów teleinformatycznych jest zobowiązany do:

1) stosowania zasad określonych w pkt IV,
2) nieudostępniania danych dostępowych do systemów informatycznych osobom nieuprawnionym, w tym domownikom
3) niepobierania danych osobowych z systemów informatycznych w celu innym niż służbowy,
4) pobierania i zapisywania tylko niezbędnych dokumentów.

VI. Obowiązki podczas spotkań zdalnych, wideokonferencji

1. Organizacja spotkań może nastąpić tylko przy użyciu dostarczonych przez pracodawcę rozwiązań informatycznych.
2. Podczas spotkań przebiegających z ujawnianiem wizerunków należy ograniczyć do minimum rejestrowanie spotkań.

3. W przypadku konieczności udostępniania konkretnych dokumentów podczas spotkań należy zamknąć używane wcześniej inne dokumenty, aplikacje, okna przeglądarek, aby udostępnić uczestnikom spotkania tylko i wyłącznie dedykowany dla nich plik.
4. Wszystkie pliki zapisywane w zespołach lub dedykowanej do tego przestrzeni w aplikacji do wideokonferencji należy cyklicznie przeglądać i usuwać po ustaniu ich przydatności.
5. Linki do wideokonferencji powinny być udostępniane tylko i wyłącznie uczestnikom spotkania, bezpiecznym kanałem komunikacji, zaproszenia powinny być kierowane wyłącznie na służbowe adresy e-mail.

Załącznik nr 1
do procedury ochrony danych osobowych w ramach pracy zdalnej
Niechlów, dnia 1 sierpnia 2023 r.

PRACA ZDALNA

Poniżej prezentujemy wyciąg z Polityki Ochrony Danych Osobowych oraz z Regulaminu Ochrony Danych Osobowych, w których zostały określone wytyczne w jaki sposób należy się zachować się podczas przetwarzania danych osobowych poza siedzibą Administratora.

I. ZBIÓR DOBRYCH PRAKTYK PRZY PRACY Z DOKUMENTACJĄ PAPIEROWĄ:

- Jeśli do pracy zdalnej wymagana jest dokumentacja papierowa należy przewieźć ją **bezpośrednio** od Administratora do miejsca wykonywania pracy zdalnej, aby uniknąć scenariusza, że zostanie nam ona skradziona.
- Dokumentację w miejscu wykonywania pracy zdalnej należy zabezpieczyć przed dostępem osób trzecich.
- Jeśli w trakcie pracy wytworzymy dokumentację wymagającą zniszczenia, a nie posiadamy niszczarki odpowiedniej klasy (niszczenie na paski węższe niż 5mm) dokumentację taką należy po zakończeniu pracy zdalnej przywieźć do Administratora i zniszczyć ją w niszczarkach

II. ZBIÓR DOBRYCH PRAKTYK PRZY PRACY Z DOKUMENTACJĄ ELEKTRONICZNĄ:

ASI – Administrator Systemu Informatycznego (lub osoba mająca uprawnienia Administratora w systemie informatycznym

- Administrator przekazuje ASI listę osób upoważnionych do pracy zdalnej.
- ASI umożliwia pracę zdalną o łącza szyfrowane.
- Osoba wykonująca pracę zdalną musi posiadać zainstalowany program antywirusowy.

- Osoba wykonująca pracę zdalną podczas aktywnej sesji musi wyłączyć zbędne programy (takie jak FB, prywatna poczta itd.)
- Podczas trwania połącznia zdalnego nie dopuszczać do pracy przy komputerze innych użytkowników.
- Osoba wykonująca pracę zdalną po zakończeniu jej wykonywania zobowiązana jest do usunięcia (także z kosza) wszystkich danych Administratora pozyskanych w trakcie świadczenia pracy zdalnej.
- Po zakończeniu pracy należy rozłączyć tunel szyfrowany (jeśli był uruchomiony)
- Po zakończeniu zdalnej pracy i powrotu do siedziby Administratora ASI, wykorzystując listę osób uprawnionych, blokuje tunele VPN.

Przypominamy
Kontakt do Inspektora Ochrony Danych (IOD)
Tomasz Wadas tel. 570 170 137
Kontakt do ASI/Informatyka
Kacper Pieczulis tel. 504 044 769
Andrzej Płaskoń tel. 509 754 048
Dominik Kozubek tel. 885 808 581

W razie wątpliwości oraz w przypadku zaistnienia incydentu należy bezzwłocznie kontaktować się z przełożonym oraz z IOD.

Naruszenie bezpieczeństwa prowadzące do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych.
naruszenie poufności, które polega na ujawnieniu lub udostępnieniu danych osobie nieuprawnionej,
naruszenie integralności, które sprowadza się do zmiany treści danych osobowych, czyli ich modyfikowania, w sposób nieautoryzowany,
naruszenie dostępności, które wiąże się z trwałą utratą dostępu do danych lub ich zniszczeniem.

III. WYCIĄG Z POLITYKI OCHRONY DANYCH OSOBOWYCH

15 OBOWIĄZEK ZACHOWANIA POUFNOŚCI

1. Każda z osób dopuszczona do przetwarzania danych osobowych jest zobowiązana do:
   a. przetwarzania danych osobowych wyłącznie w zakresie i celu przewidzianym w upoważnieniu wydanym przez ADO,
   b. zachowania w tajemnicy danych osobowych do których posiada dostęp w związku z wykonywaniem zadań powierzonych przez ADO,
   c. niewykorzystywania danych osobowych w celach niezgodnych z zakresem i celem powierzonych zadań przez ADO,
   d. zachowania w tajemnicy sposobów zabezpieczenia danych osobowych,

e. ochrony danych osobowych przed przypadkowym lub niezgodnym z prawem zniszczeniem, utratą, modyfikacją, nieuprawnionym ujawnieniem, nieuprawnionym dostępem oraz przetwarzaniem.

IV. WYCIĄG REGULAMINU OCHRONY DANYCH OSOBOWYCH

3 ZASADY UŻYTKOWANIA SPRZĘTU KOMPUTEROWEGO, NOŚNIKÓW I PROGRAMÓW

1. Sprzęt komputerowy powinien zawsze być pod nadzorem osób, którym został powierzony.
2. Jeśli komputer przenośny (na których przetwarzane są dane osobowe lub łączące się za pomocą VPN z aplikacjami przetwarzającymi dane osobowe) zostanie zgubiony, skradziony użytkownik tego sprzętu powinien jak najszybciej powiadomić o tym fakcie ADO oraz ASI.
3. W przypadku konieczności instalacji dodatkowego oprogramowania należy zwrócić się do ASI, w przypadku instalacji dodatkowych komponentów ASI decyduje, czy montaż dokona samodzielnie czy przy wsparciu zewnętrznej firmy. Dokonywanie samodzielnie jakichkolwiek zmian w konfiguracji sprzętu IT jest zabronione.
4. Wykonywanie jakichkolwiek napraw sprzętu komputerowego przez użytkownika jest zabronione.
5. Polityka czystego ekranu – monitory powinny zostać tak ustawione by nie było możliwości przypadkowego lub celowego odczytania informacji wyświetlanych na tym monitorze. Należy zwrócić szczególną uwagę na stanowiska komputerowe zlokalizowane na parterze np. skierowane w stronę okna. Użytkownik komputera zobowiązany jest do takiego ustawienia monitora ekranowego, aby uniemożliwić odczyt prezentowanych na nim informacji osobom nieuprawnionym.
6. Przed opuszczeniem stanowiska pracy, użytkownik zobowiązany jest wywołać blokowany hasłem wygaszacz ekranu (klawisz WINDOWS+L) lub wylogować się z systemu bądź z programu.
7. Po zakończeniu pracy użytkownik systemu zobowiązany jest zamknąć wszystkie używane programy (wylogować się) i system operacyjny (wyłączyć komputer) oraz zabezpieczyć nośniki informacji, na których znajdują się dane osobowe.
8. Dane osobowe znajdujące się na dysku lub nośniku współużytkowanym mogą zostać udostępnione wyłącznie osobom posiadającym stosowne upoważnienia.
9. Użytkownik nie ma prawa do instalowania na komputerze żadnego oprogramowania ani uruchamiania nieznanych programów, które nie wymagają instalacji.
10. Użytkownik nie ma prawa wykorzystywać do wypełniania obowiązków pracowniczych własnego sprzętu komputerowego a w szczególności podłączać go do lokalnej sieci komputerowej.
11. Usuwanie danych osobowych z urządzeń, dysków lub innych nośników informatycznych przeprowadza się zgodnie z Załącznikiem C - Procedury 2a - Procedurą zniszczenia nośników komputerowych.
12. Urządzenia, dyski lub inne informatyczne nośniki zawierające dane osobowe przeznaczone do likwidacji, pozbawia się wcześniej zapisu tych danych zgodnie z Załącznikiem C - Procedury 2a - Procedurą zniszczenia nośników komputerowych a w przypadku, gdy nie jest to możliwe, uszkadza się je w sposób uniemożliwiający ich odczytanie.
13. Urządzenia, dyski lub inne informatyczne nośniki zawierające dane osobowe, przeznaczone do przekazania innemu podmiotowi, nieuprawnionemu do

otrzymywania danych osobowych pozbawia się wcześniej zapisu tych danych zgodnie z Załącznikiem C - Procedury 2b – Procedurą usunięcia danych osobowych.

14. Uszkodzone urządzenia zawierające dane osobowe naprawia się pod nadzorem osoby upoważnionej, a przed przekazaniem do naprawy w serwisie zewnętrznym pozbawia się zapisu tych danych - w przypadku, gdy nie jest to możliwe przekazanie urządzenia do serwisu poprzedzane jest podpisaniem umowy o powierzeniu danych osobowych.
15. Szczegółowe zasady przekazywania uszkodzonego sprzętu komputerowego do serwisu określone zostały w Załącznikiem C - Procedury 5 – Procedura napraw w serwisach zewnętrznych.

4 UŻYTKOWANIE KOMPUTERÓW PRZENOŚNYCH

1. W przypadku konieczności wyniesienia komputera przenośnego zawierającego dane osobowe poza obszar przetwarzania danych określony w Polityce ochrony danych osobowych Użytkownik zobowiązany jest do przechowywania tych danych w postaci zaszyfrowanej (zakodowany dysk, folder lub plik) z zastosowaniem hasła o minimalnej długości 8 znaków (duże, małe litery, znaki specjalne i cyfry) oraz szyfrowania o minimalnej długości klucza 256 bitów.
2. Zabronione jest przechowywanie danych osobowych na komputerach przenośnych, do których dostęp mają osoby nieupoważnione nawet w przypadku stałej obserwacji urządzenia przez osobę uprawnioną (np. pokazy i prezentacje multimedialne).
3. W przypadku kradzieży lub zgubienia komputera przenośnego, Użytkownik powinien natychmiast powiadomić o tym ADO lub IOD, zaznaczając jednocześnie, jakiego rodzaju dane były na tym urządzeniu przechowywane.
4. Użytkownik zobowiązany jest do zabezpieczenia komputera przenośnego w czasie transportu.
5. W przypadku, gdy komputer przenośny pozostawiony jest w miejscu dostępnym dla osób nieupoważnionych, Użytkownik jest zobowiązany do stosowania kabla zabezpieczającego, np. podczas konferencji, prezentacji, szkoleń, targów itp.
6. Użytkownik komputera przenośnego zawierającego dane osobowe jest zobowiązany do regularnego tworzenia kopii bezpieczeństwa danych na serwerze lub na określonych nośnikach (pendrive, CD, DVD). Nośniki z takimi kopiami powinny być przechowywane w bezpiecznym miejscu, z uwzględnieniem ochrony przed dostępem osób niepowołanych.
7. Za przygotowanie mechanizmów umożliwiających zabezpieczanie danych osobowych przechowywanych na urządzeniach mobilnych lub dyskach lokalnych komputerów odpowiedzialny jest ASI.
8. W przypadku używania komputera przenośnego zawierającego dane osobowe poza obszarem przetwarzania danych lub logowania się do stron internetowych wymagających podania loginu i hasła nie wolno korzystać z publicznych sieci bezprzewodowych (w restauracjach, hotelach, kawiarniach itp.)

5 ZASADY POSŁUGIWANIA SIĘ HASŁAMI

1. Hasło użytkownika utrzymuje się w tajemnicy również po upływie jego ważności.
2. Użytkownicy są odpowiedzialni za zachowanie poufności swoich haseł - haseł nie należy przechowywać w postaci zapisanej w najbliższym otoczeniu stanowiska pracy.
3. Hasło należy wprowadzać w sposób, który uniemożliwia innym osobom jego poznanie.
4. Przy wyborze hasła obowiązują następujące zasady:
   a) minimalna długość hasła dla komputerów/laptopów wynoszonych poza siedzibę Administratora - 12 znaków,
   b) zakazuje się stosować:
      - haseł, które użytkownik stosował uprzednio w okresie minionych 12 m-cy,
      - swojego identyfikatora w jakiejkolwiek formie (np. pisanej dużymi literami, w odwrotnym porządku, dublując każdą literę itp.),
      - swojego imienia, drugiego imienia, nazwiska, przezwiska, pseudonimu w jakiekolwiek formie,
      - imion, w szczególności imion osób z najbliżej rodziny,
      - ogólnie dostępnych informacji o użytkowniku tak jak: numer telefonu, numer rejestracyjny samochodu, marka samochodu, numer dowodu osobistego, nazwa ulicy, na której mieszka lub pracuje itp.,
      - wyrazów słownikowych,
      - przewidywalnych sekwencji znaków z klawiatury np. „QWERTY", „123456789" itp.
   c) należy stosować:
      - hasła zawierające małe i duże litery,
      - hasła zawierające kombinacje liter i cyfr,
      - hasła zawierające znaki specjalne: znaki interpunkcyjne, nawiasy, symbole @, # itp.,
      - hasła, które można zapamiętać bez zapisywania,
      - hasła łatwe i szybkie do wprowadzenia, po to aby trudniej było podejrzeć je osobom trzecim.
      - Jeśli system tego nie wymusi zmieniać hasło tymczasowe uzyskane od ASI.
5. Hasło należy wprowadzać w sposób, który uniemożliwia innym osobom jego poznanie.
6. W sytuacji, kiedy zachodzi podejrzenie, że ktoś poznał hasło, użytkownik zobowiązany jest natychmiast je zmienić.
7. Jeżeli system informatyczny posiada mechanizm wymuszania okresowej zmiany haseł oraz blokady dostępu użytkownika po kilku (maksymalnie sześciu) nieudanych próbach logowania ASI musi uaktywnić te funkcjonalności.
8. Hasła należy zmieniać nie rzadziej niż co 30 dni.
9. Jeżeli system operacyjny nie posiada mechanizmu wymuszania okresowej zmiany hasła użytkownik zobowiązany jest do jego zmiany.
10. W sytuacji, kiedy zachodzi podejrzenie, że ktoś poznał hasło w sposób nieuprawniony, użytkownik zobowiązany jest powiadomić o tym fakcie ASI oraz natychmiast zmienić hasło.
11. Zmiany hasła nie wolno zlecać innym osobom. W przypadku utracenia hasła użytkownik ma obowiązek skontaktować się z ASI.
12. Zabrania się korzystania w systemach, które to umożliwiają, z opcji zapamiętania nazw użytkownika lub jego hasła.

13. ASI przekazuje nowemu pracownikowi hasło w kopercie a osoba odbierająca hasło potwierdza jego odbiór na wniosku o nadanie uprawnień.
14. Hasło ustanowione podczas przyznawania uprawnień należy zmienić na indywidualne podczas pierwszego logowania się w systemie informatycznym.

6 ZABEZPIECZANIE DOKUMENTACJI W WERSJI PAPIEROWEJ

1. Przetwarzając dane osobowe w wersji papierowej należy zabezpieczyć je przed przypadkowym zniszczeniem, udostępnieniem, sfotografowaniem.
2. Dokumenty papierowe zawierające dane osobowe przeznaczone do likwidacji są niszczone przy wykorzystaniu niszczarek lub niszczone przez firmy zajmujące się niszczeniem dokumentów.
3. Pozostawienie dokumentów zawierających dane osobowe w pomieszczeniach ogólnodostępnych lub urządzeniach (np. kserokopiarkach) jest możliwe wyłącznie w przypadku zastosowania zabezpieczeń uniemożliwiających dostęp osób nieuprawnionych do tych dokumentów.
4. Zabrania się wyrzucania jakichkolwiek dokumentów bez ich wcześniejszego zniszczenia w sposób uniemożliwiający odczytanie ich treści.
5. W przypadku używania urządzeń służących do kopiowania dokumentów (kserokopiarka, skaner, urządzenie wielofunkcyjne itp.) po skończonej czynności kopiowania pracownik sprawdza czy nie pozostawił dokumentu w urządzeniu oraz zabiera ze sobą wszystkie kopie, w tym również nieprawidłowo wykonane. Za właściwe zabezpieczenie dokumentów podczas kopiowania odpowiada pracownik wykonujący te czynności.

7 ZASADY KORZYSTANIA Z NOŚNIKÓW DANYCH

1. Wynoszenie nośników zawierających dane osobowe (np. pamięci USB, płyty CD/DVD) poza obszar przetwarzania danych osobowych jest dozwolone wyłącznie za zgodą Administratora Danych Osobowych.
2. Dane osobowe wynoszone poza obszar przetwarzania należy zaszyfrować z zastosowaniem hasła o minimalnej długości 12 znaków (duże, małe litery, znaki specjalne i cyfry) oraz klucza o minimalnej długości 256 bitów.
3. W sytuacji, gdy zaistnieje konieczność przetransportowania dokumentów (akt) zawierających dane osobowe poza obszar przetwarzania danych czynność tę wykonuje pracownik posiadający upoważnienie do przetwarzania danych osobowych. Dokument w trakcie drogi musi być zabezpieczony przed dostępem osób nieupoważnionych lub kradzieżą a transport odbywa się najkrótszą drogą.

8 ZASADY KORZYSTANIA Z SIECI INTERNET

1. Sieć Internet można wykorzystywać wyłącznie do celów z wiązanych z wykonywaniem obowiązków służbowych.
2. Dane osobowe mogą być przesyłane za pośrednictwem sieci Internet (np. dyski internetowe) wyłącznie przez osoby upoważnione przez ADO z wykorzystaniem mechanizmów kryptograficznych (hasła o minimalnej długości 12 znaków i szyfrowanie o minimalnej długości klucza 256 bitów).

3. Instalowanie jakichkolwiek programów pobranych z Internetu jest możliwe wyłącznie za zgodą ASI.
4. Użytkownik ponosi pełną odpowiedzialność za wszystkie szkody powstałe w systemie informatycznym na skutek działania programu samodzielnie pobranego przez tego użytkownika.
5. Przeglądarka internetowa musi mieć wyłączoną opcję zapamiętywania haseł i automatycznego uzupełniania formularzy – użytkownik systemu nie może dokonywać samodzielnej modyfikacji tych ustawień.
6. Zabrania się umieszczania w Internecie treści powszechnie uznawanych za obraźliwe. Zabrania się przeglądania stron internetowych zawierających materiały erotyczne, pornograficzne oraz opisujących sposoby łamania prawa i zabezpieczeń systemów informatycznych - Administrator Danych Osobowych może wprowadzić środki techniczne gwarantujące blokadę (filtrowanie) takich witryn i treści.
7. Nie należy przeglądać stron internetowych, po otwarciu których pojawi się komunikat o możliwości zainfekowania komputera lub żądanie podania informacji niezwiązanych z przeglądaną witryną (kody, hasła, dane służące do uwierzytelniania).
8. Należy informować ASI o wszystkich przypadkach pojawienia się komunikatu o nieprawidłowym (niezaufanym) certyfikacie podczas przeglądania stron internetowych, które zaczynają się od frazy „https:".
9. Należy zachować szczególną ostrożność w przypadku logowania się na stronach internetowych banków, sklepów i poczty elektronicznej – w przypadku nieoczekiwanej zmiany ich wyglądu, problemów z zalogowaniem się lub informacji o nieprawidłowym certyfikacie należy bezwzględnie powiadomić ASI.

9 ZASADY KORZYSTANIA Z POCZTY ELEKTRONICZNEJ

1. Pocztę elektroniczną należy wykorzystywać wyłącznie do celów służbowych.
2. Dane osobowe mogą być przesyłane za pośrednictwem poczty elektroniczne wyłącznie przez osoby upoważnione przez ADO z wykorzystaniem mechanizmów kryptograficznych (hasła o minimalnej długości 12 znaków i szyfrowanie o minimalnej długości klucza 256 bitów).
3. Hasło umożliwiające odszyfrowanie danych osobowych jeśli istnieje taka możliwość należy przekazywać innym kanałem komunikacji (np. telefonicznie lub sms-em).
4. Należy ograniczyć otwieranie załączników do poczty elektronicznej otrzymanej od nieznanych nadawców. Często są to informacje o niezapłaconej fakturze, zmianie terminu dostawy paczki.
5. Nie należy otwierać załączników do poczty elektronicznej od nadawców posługujących się adresem zbliżonym do powszechnie znanego (poczta, banki, dostawcy mediów) w przypadku gdy nie oczekujemy takiej przesyłki.
6. Nie należy otwierać zaszyfrowanych załączników do poczty elektronicznej, plików spakowanych (zazwyczaj pliki o nazwach zakończonych .zip lub .rar .7z .tar) oraz nieznanych linków występujących w jej treści w przypadku gdy nie oczekujemy na taką przesyłkę.
7. W celu potwierdzenia wiarygodności takiego mail-a można podjąć próbę kontaktu z jego nadawcą za pośrednictwem telefonu lub poczty elektronicznej – w przypadku przesyłek zawierających złośliwy kod jego nadawca zazwyczaj nie istnieje.
8. Wszystkie podejrzane e-maile należy bezwzględnie zgłaszać ASI.
9. Przy wysyłaniu poczty elektronicznej do kilku adresatów jednocześnie należy przy ich adresach stosować opcję UDW „Ukryty Do Wiadomości:"

10. Zakazuje się wysyłania korespondencji służbowej na prywatne skrzynki pocztowe pracowników lub innych osób za wyjątkiem sytuacji, w których przepis obowiązującego prawa stanowi inaczej.

10 OCHRONA ANTYWIRUSOWA

1. Wszystkie stacje robocze chronione są przez program antywirusowy.
2. ASI jest odpowiedzialny za instalację i aktualizację oprogramowania antywirusowego.
3. Jakakolwiek ingerencja w oprogramowanie antywirusowe ze strony użytkownika systemu jest niedozwolona.
4. Każdorazowe użycie pamięci zewnętrznej (nośnika danych) musi być poprzedzone pełnym przeskanowaniem takiego nośnika za pomocą oprogramowania antywirusowego – za przeprowadzenie skanowania odpowiedzialny jest użytkownik, który zamierza użyć pamięci zewnętrznej.
5. Użytkownik zobowiązany jest natychmiast powiadomić ASI w przypadku wykrycia wirusa.
6. W przypadku wykrycia wirusów komputerowych ASI sprawdza wszystkie stanowiska komputerowe, posiadane nośniki oraz dyski sieciowe.

Załącznik Nr 3
do Zarządzenia Nr 97/2023
Wójta Gminy Niechlów
z dnia 1 sierpnia 2023 r.

Protokół zdawczo-odbiorczy z dnia .....

Przekazujący: .....
(Imię i nazwisko osoby reprezentującej pracodawcę)

Przyjmujący: .....
(Imię i Nazwisko oraz stanowisko służbowe pracownika)

§ 1.

Przedmiot przekazania stanowi sprzęt komputerowy o numerze seryjnym/inwentarzowym:

.....

§ 2.

Sprzęt komputerowy wymieniony w § 1 przekazywany jest przyjmującemu.

§ 3.

Przyjmujący stwierdza, że stan przekazanego mienia nie budzi zastrzeżeń.

§ 4.

Protokół sporządzono w dwóch jednobrzmiących egzemplarzach, po jednym dla każdej ze stron.

Przekazujący

.....
(podpis)

Przyjmujący

.....
(podpis)

Załącznik Nr 4
do Zarządzenia Nr 97/2023
Wójta Gminy Niechlów
z dnia 1 sierpnia 2023 r.

..... Niechlów, ...
(imię i nazwisko pracownika)

.....
(stanowisko)

Ewidencja wykonywanych czynności w okresie pracy zdalnej
od dnia ..... do dnia .....

Lp.	Data	Rodzaj pracy/opis czynności

.....
(podpis pracownika)

Załącznik Nr 5
do Zarządzenia Nr 97/2023
Wójta Gminy Niechlów
z dnia 1 sierpnia 2023 r.

O ś w i a d c z e n i e

Oświadczam, że zapoznałem/am się z treścią Zarządzenia Nr 97/2023 Wójta Gminy Niechlów z dnia 1 sierpnia 2023 r. w sprawie organizowania pracy zdalnej okazjonalnej w Urzędzie Gminy Niechlów.