

**Zarządzenie Nr 335 /23 Wójta Gminy Nowa Ruda z dnia 10 sierpnia 2023 roku
w sprawie wprowadzenia Regulaminu Pracy zdalnej oraz Procedur ochrony
danych osobowych w ramach pracy zdalnej w Urzędzie Gminy Nowa Ruda**

Na podstawie art. 30 ust. 3 i ust. 5 ustawy z dnia 8 marca 1990 roku o samorządzie gminnym (Dz. U. z 2023 r. poz. 40 z późn. zm.), w związku z art. 67²⁰ oraz 67²⁶ ustawy z dnia 26 czerwca 1974 r. Kodeks pracy (Dz.U.2023.1465 t.j. ze zmianami).

Wójt Gminy Nowa Ruda zarządza, co następuje:

2. Wprowadza się Regulamin Pracy zdalnej oraz Procedury pracy zdalnej w Urzędzie Gminy Nowa Ruda w brzmieniu określonym w załączniku nr 1 i nr 2 do niniejszego zarządzenia.

§3. Wykonanie Zarządzenia powierza się Kierownikowi Referatu Organizacyjnemu, Spraw Obywatelskich i Zarządzania Kryzysowego.

§4. Zarządzenie wchodzi w życie z dniem wydania.

/Adrianna Mierzejewska – Wójt Gminy Nowa Ruda/

Załącznik nr 1 do zarządzenia Nr 335 /23

Wójta Gminy Nowa Ruda

z dnia 10 sierpnia 2023 r.

REGULAMIN PRACY ZDALNEJ

W

Urzędzie Gminy Nowa Ruda

2023

§ 1.

Postanowienia ogólne

1. Na podstawie art. 67²⁰ Kodeksu Pracy, w Urzędzie Gminy Nowa Ruda ustala się regulamin pracy zdalnej określający zasady wykonywania przez pracownika pracy w formie zdalnej oraz związane z tym prawa i obowiązki Pracodawcy i Pracownika.
2. Ilekroć w Regulaminie jest mowa o:
 - **Pracodawcy** – należy przez to rozumieć Urząd Gminy Nowa Ruda.
 - **Pracownika** – należy przez to rozumieć osobę zatrudnioną w oparciu o umowę o pracę.
 - **Pracy zdalnej** – należy przez to rozumieć pracę wykonywaną całkowicie lub częściowo w miejscu wskazanym przez pracownika i każdorazowo uzgodnionym z pracodawcą, w tym pod adresem zamieszkania pracownika, w szczególności z wykorzystaniem środków bezpośredniego porozumiewania się na odległość.
 - **Okazjonalnej pracy zdalnej** - należy przez to rozumieć pracę wykonywaną częściowo w miejscu wskazanym przez pracownika i każdorazowo uzgodnionym z pracodawcą, w tym pod adresem zamieszkania pracownika, w szczególności z wykorzystaniem środków bezpośredniego porozumiewania się na odległość, w wymiarze nieprzekraczającym 24 dni w roku kalendarzowym.

§ 2.

Grupy pracowników objęte pracą zdalną

1. Pracodawca dopuszcza możliwość wykonywania pracy zdalnej dla Pracowników zatrudnionych na stanowiskach:
 - a) Wójt
 - b) Z-ca Wójta
 - c) Sekretarz gminy
 - d) Skarbnik gminy
 - e) Radca prawny
 - f) Kierownik referatu
 - g) pracownicy administracyjno-biurowi
2. Pracownicy zatrudnieni na wszystkich stanowiskach pracy mogą wykonywać pracę zdalną

okazjonalną do 24 dni w roku kalendarzowym, na podstawie wniosku pracownika w tym zakresie i za zgodą pracodawcy.

§ 3.

Formy pracy zdalnej

1. Pracodawca przewiduje możliwość wykonywania przez uprawnionych pracowników pracy zdalnej w następujących formach:
 - a) częściowa
 - b) całościowa
 - c) okazjonalna
2. Pracownik uprawniony do wykonywania pracy zdalnej nie ma w tym zakresie roszczenia wobec pracodawcy i może świadczyć pracę w tej formie, wyłącznie za zgodą pracodawcy lub w określonych przypadkach na jego polecenie.
3. Pracodawca udziela zgody na pracę zdalną poszczególnym pracownikom biorąc pod uwagę obiektywne kryteria związane organizacją pracy i rodzajem pracy wykonywanej przez uprawnionego pracownika.

§ 4.

Procedura polecania-udzielania zgody na pracę zdalną

1. Uprawniony pracownik składa wniosek o wykonywanie pracy zdalnej lub okazjonalnej pracy zdalnej w formie pisemnej papierowej lub elektronicznej najpóźniej w dniu poprzedzającym dzień, w którym pracownik zamierza rozpocząć wykonywanie pracy zdalnej.
2. W szczególnie uzasadnionych przypadkach pracodawca może wyrazić zgodę na pracę zdalną na wniosek złożony w tym samym dniu, na który przypada jej rozpoczęcie.
3. We wniosku pracownik wskazuje każdorazowo miejsce świadczenia pracy zdalnej, którego pracownik nie może zmienić bez uprzedniej zgody pracodawcy.
4. Polecenie pracownikowi świadczenia pracy zdalnej, w przypadkach wynikających z przepisów powszechnych, może nastąpić w dowolnej formie, która umożliwia pracownikowi zapoznanie się z tym poleceniem.
5. Do wyrażania zgód na pracę zdalną, jak również wydawania poleceń pracy zdalnej

pracodawca może upoważnić kierowników wydzielonych komórek organizacyjnych lub bezpośrednich przełożonych pracowników.

6. Dopuszcza się możliwość świadczenia pracy zdalnej lub polecenie pracy zdalnej na część godzin pracy pracownika wynikającej z obowiązującego go dobowego wymiaru czasu pracy.

§ 5.

Ogólne zasady pracy zdalnej

1. Pracownik wykonuje pracę zdalną w godzinach pracy wynikających z obowiązującego go systemu i rozkładu czasu pracy.
2. Pracownik wykonuje pracę zdalną zgodnie z posiadanym zakresem obowiązków na zajmowanym stanowisku pracy.
3. Praca zdalna może być wykonywana częściowo (w niektórych dniach, przez czas określony, w niektórych godzinach) poza miejscem stałego jej wykonywania wynikającym z umowy o pracę.
4. Pracownik wykonujący pracę zdalną ma prawo do przebywania na terenie zakładu pracy, kontaktowanie się z innymi pracownikami oraz korzystanie z pomieszczeń i urządzeń pracodawcy, zakładowych obiektów socjalnych na zasadach przyjętych dla ogółu pracowników.
5. Zmiana miejsca wykonywania pracy zdalnej wymaga każdorazowo zgody pracodawcy.
6. Wykonywanie pracy zdalnej w innym niż uzgodnione i zaakceptowane przez pracodawcę miejscu, stanowi ciężkie naruszenie podstawowych obowiązków pracowniczych.

§ 6.

Zasady porozumiewania się pracodawcy i pracownika wykonującego pracę zdalną

1. Pracownik wykonujący pracę zdalną i pracodawca przekazują informacje niezbędne do wzajemnego porozumiewania się za pomocą środków bezpośredniego porozumiewania się na odległość.
2. Osobą odpowiedzialną za współpracę z pracownikiem wykonującym pracę zdalnie jest bezpośredni przełożony pracownika.
3. Pracownik jest obowiązany potwierdzać w każdym dniu wykonywania pracy zdalnej obecność na stanowisku pracy poprzez: e-mail, telefon.

§ 7.

Prawa i obowiązki pracownika wykonującego pracę zdalną

1. Pracownik wykonujący pracę zdalną jest zobowiązany do przestrzegania:
 - zasad ochrony przed zagrożeniami wynikającymi z oceny ryzyka zawodowego przy pracy zdalnej,
 - procedury ochrony danych osobowych przy pracy zdalnej,
2. informacji (instrukcji bhp) w zakresie wykonywania pracy zdalnej.
3. Pracownik wykonujący pracę zdalną jest zobowiązany do złożenia przed rozpoczęciem pracy zdalnej oświadczenia w formie pisemnej papierowej lub elektronicznej.
4. Pracownik zobowiązuje się do używania udostępnionych mu materiałów, narzędzi w tym urządzeń technicznych, oprogramowania wyłącznie do celów służbowych, w sposób zgodny z ich przeznaczeniem.
5. Pracownik wykonujący pracę zdalną jest zobowiązany do dbania o powierzone mu celem wykonywania pracy zdalnej mienie pracodawcy oraz jego właściwe zabezpieczenie po godzinach pracy.
6. Pracownik jest zobowiązany do wykonywania pracy zgodnie z treścią umowy łączącej go z pracodawcą oraz zakresem obowiązków.
7. Ponadto pracownik zobowiązuje się do ewidencji pracy.

§ 8.

Prawa i obowiązki pracodawcy

1. Pracodawca jest obowiązany zapewnić pracownikowi wykonującemu pracę zdalną materiały i narzędzia pracy, w tym urządzenia techniczne, niezbędne do wykonywania pracy zdalnej lub wypłacać ekwiwalent za wykorzystywanie przez pracownika wykonującego pracę zdalną materiałów i narzędzi pracy, w tym urządzeń technicznych, niezbędnych do wykonywania pracy zdalnej, niezapewnionych przez Pracodawcę.
2. Pracodawca zapewnia niezbędne przeszkolenie pracownika w zakresie obsługi oprogramowania oraz środków łączności przed przystąpieniem pracownika do pracy zdalnej.
3. Przed dopuszczeniem do wykonywania pracy zdalnej pracodawca zapozna pracownika z oceną ryzyka zawodowego oraz informacją zawierającą zasady bezpiecznego i higienicznego wykonywania pracy zdalnej, jak również procedurą ochrony danych osobowych przy pracy zdalnej.

4. Pracodawca nie odpowiada za stan pomieszczeń pracy, obiektów budowlanych, w których jest wykonywana praca oraz pomieszczeń i urządzeń higieniczno-sanitarnych oraz inne przepisy z zakresu bezpieczeństwa i higieny pracy, dla których wyłącznie stosowania przy pracy zdalnej wynika z powszechnie obowiązujących przepisów w tym zakresie.

§ 9.

Techniczna aspekty pracy zdalnej

1. Pracodawca zapewnia w pełnym zakresie instalację, inwentaryzację, konserwację, aktualizację oprogramowania i serwis powierzonych pracownikowi narzędzi pracy, w tym urządzeń technicznych.
2. Pracownik ma prawo do wsparcia technicznego ze strony pracodawcy. Pracownik niezwłocznie zgłasza pracodawcy wszelkie uzasadnione potrzeby w tym zakresie.
3. Pracownik informuje o problemie technicznym pracodawcę.
4. W przypadku konieczności dokonania instalacji, inwentaryzacji, konserwacji, aktualizacji oprogramowania i serwisu powierzonych pracownikowi narzędzi pracy, w tym urządzeń technicznych, pracownik jest zobowiązany do niezwłocznego poinformowania pracodawcy w tym zakresie – nie może samodzielnie, bez zgody pracodawcy podejmować jakichkolwiek czynności z tym związanych.
5. Pracownik jest zobowiązany umożliwić pracodawcy lub osobom przez niego uprawnionym dokonanie instalacji, inwentaryzacji, konserwacji, aktualizacji oprogramowania i serwisu powierzonych pracownikowi narzędzi pracy, w tym urządzeń technicznych poprzez ich udostępnienie w sposób uzgodniony z pracodawcą, bezpośrednim przełożonym lub pracownikiem odpowiedzialnym za wykonanie tych czynności.

§ 10.

Koszty, ekwiwalent, ryczałt

1. Pracodawca pokrywa pracownikowi wykonującemu pracę w formie zdalnej koszty:
 - energii elektrycznej,
 - niezbędnych usług telekomunikacyjnych. – o ile nie zapewniono dostępu do tych usług w inny sposób.
2. W przypadku wykorzystywania przez pracownika w okresie pracy zdalnej materiałów i narzędzi pracy, w tym urządzeń technicznych, niezbędnych do wykonywania tej pracy, niezapewnionych przez pracodawcę, pracownikowi przysługuje ekwiwalent pieniężny.
3. Koszty pracy zdalnej ponoszone przez pracownika oraz ekwiwalent za używanie własnych

materiałów i narzędzi pracy w tym urządzeń technicznych przez pracownika zostaną zrekompensowane wypłatą ryczałtu.

4. Pracownik, który przebywał przez wszystkie dni robocze danego miesiąca kalendarzowego na usprawiedliwionej nieobecności w pracy, nie przysługuje zwrot kosztów albo ryczałt za ten miesiąc.
5. Pracownikowi zatrudnionemu w niepełnym wymiarze czasu pracy wysokość zwrotu kosztów lub ryczałtu ustala się proporcjonalnie do jego wymiaru czasu pracy.
6. Uprawnienie do zwrotu kosztów albo ryczałtu za pracę zdalną ustala się na podstawie uzgodnień z pracodawcą.
7. Pracownikowi przebywającemu na okazjonalnej pracy zdalnej do 24 dni w roku kalendarzowym nie przysługuje zwrot kosztów ani ryczałt z tytułu pracy zdalnej.

§ 11.

Zasady kontroli pracy zdalnej

1. Pracodawca ma prawo, w miejscu wykonywania pracy zdalnej i w godzinach pracy pracownika, przeprowadzać:
 - kontrolę wykonywania pracy zdalnej przez pracownika,
 - kontrolę w zakresie bezpieczeństwa i higieny pracy
 - kontrole w zakresie przestrzegania wymogów bezpieczeństwa i ochrony informacji, w tym procedur ochrony danych osobowych.
2. Termin kontroli pracodawca ustala w porozumieniu z pracownikiem, najpóźniej dzień przed jej przeprowadzeniem.
3. Kontrola jest przeprowadzana w godzinach pracy pracownika wynikających z jego rozkładu czasu pracy w dniu kontroli.
4. Kontrole przeprowadza się w obecności pracownika.
5. Osobami upoważnionymi do przeprowadzania kontroli w miejscu wykonywania pracy, są: pracodawca, osoba upoważniona.
6. Pracownik przed rozpoczęciem kontroli jest informowany o osobie lub osobach, które będą przeprowadzać kontrolę wykonywanej przez pracownika pracy w formie zdalnej.
7. Osoby kontrolujące są zobowiązane do prowadzenia czynności kontrolnych w sposób nienaruszających prywatności pracownika wykonującego pracę zdalną i innych osób obecnych w czasie kontroli.

8. Osoby kontrolujące nie mogą utrudniać korzystania z pomieszczeń domowych pracownika zdalnego w sposób zgodny z ich przeznaczeniem.
9. Pracodawca dostosowuje sposób przeprowadzania kontroli do miejsca wykonywania pracy zdalnej i jej rodzaju.
10. Kontrola pracy zdalnej nie obejmuje zagadnień z zakresu bezpieczeństwa i higieny pracy w zakresie wyłączonym powszechnie obowiązującymi przepisami prawa pracy w tym zakresie.

§ 12.

Postanowienia końcowe

1. Regulamin wchodzi w życie po upływie 2 tygodni od dnia podania go do wiadomości Pracowników poprzez wywieszenie na tablicy ogłoszeń Urzędu Gminy Nowa Ruda.
2. W sprawach nieuregulowanych niniejszym Regulaminem zastosowanie znajdują powszechnie obowiązujące przepisy w tym zakresie.
3. Przed przystąpieniem do wykonywania pracy zdalnej pracownik zapoznaje z treścią niniejszego Regulaminu, co potwierdza pisemnym lub elektronicznym oświadczeniem i zobowiązaniem do jego przestrzegania

.....

(imię i nazwisko pracownika)

Oświadczam, że w dniu zapoznałem się z zapisami Regulaminu Pracy
Zdalnej i zobowiązuję się do jego stosowania.

.....

(data)

.....

(czytelny podpis)

Załącznik nr 2 do zarządzenia Nr 335/23

Wójta Gminy Nowa Ruda

z dnia 10 sierpnia 2023 r.

Procedura bezpiecznego przetwarzania danych osobowych w pracy zdalnej w Urzędzie Gminy Nowa Ruda

Celem niniejszej procedury jest zapewnienie bezpiecznego procesu przetwarzania danych osobowych w pracy zdalnej zgodnie z 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) – dalej „RODO” oraz ustawą z dnia 10 maja 2018 o ochronie danych osobowych (Dz. U. 2019 poz. 1789).

§ 1

Postanowienia ogólne

Pracownik jest zobowiązany do świadczenia pracy zdalnej po wydaniu przez pracodawcę polecenia w postaci papierowej lub elektronicznej dotyczącej wykonywania pracy zdalnej.

Pracownik, któremu wydano polecenie pracy zdalnej zobowiązany jest w jej trakcie do przetwarzania danych osobowych zgodnie z przepisami powszechnie obowiązującego prawa, w szczególności z przepisami o ochronie danych osobowych oraz innymi przepisami regulującymi pracę Urzędu Gminy Nowa Ruda, zwłaszcza z Polityką Bezpieczeństwa Informacji, w tym Instrukcja Zarządzania Systemem Informatycznym, oraz Rejestr czynności przetwarzania, Rejestr kategorii czynności przetwarzania, Regulaminem funkcjonowania monitoringu wizyjnego.

W ramach pracy zdalnej pracownik zobowiązany jest do przetwarzania udostępnionych mu danych osobowych jedynie w celach służbowych, określonych w umowie o pracę.

Zabronione jest wykorzystywanie przez pracownika udostępnionych mu danych osobowych w celach niezwiązanych z wykonywaniem zadań i obowiązków służbowych.

Wykonywanie pracy w formie zdalnej odbywa się na służbowym lub prywatnym sprzęcie komputerowym, za pisemną zgodą pracodawcy.

W przypadku, gdy jest to konieczne dopuszcza się dostęp do sieci komputerowej Administratora dla pracowników wykonujących pracę zdalną.

§ 2

Bezpieczeństwo obszaru przetwarzania

Pracownik jest odpowiedzialny za właściwe zabezpieczenie danych osobowych przetwarzanych przez niego w ramach pracy zdalnej.

Pracownik zobowiązany jest do zachowania poufności informacji, w szczególności podczas służbowych rozmów telefonicznych lub wideokonferencji.

Pracownik zobowiązany jest do zabezpieczania dostępu do posiadanych danych służbowych przed osobami postronnymi, w tym wspólnie z nim zamieszkującymi oraz przed ich nieuprawnionym zniszczeniem lub modyfikacją.

Pracownik zobowiązany jest do uniemożliwienia wglądu osobom postronnym w treści wyświetlanej na ekranie sprzętu komputerowego, na przykład poprzez odpowiednie ustawienie ekranu lub zastosowanie nakładki na ekran tzw. filtru /folii prywatyzującej.

Pracownik zobowiązany jest do stosowania polityki czystego ekranu, tj. blokowania sprzętu komputerowego w razie oddalenia się od miejsca pracy.

Pracownik zobowiązany jest po zakończeniu pracy na sprzęcie elektronicznym każdorazowo wylogować się z programów wykorzystywanych do pracy zdalnej oraz z systemu.

Pracownik zobowiązuje się do bezpiecznego przechowywania danych osobowych zawartych w dokumentacji w formie papierowej, na przykład w szafach zamykanych na klucz.

§ 3

Bezpieczeństwo domowej sieci

1. Sprzęt komputerowy zaleca się aby był podłączony do zabezpieczonej domowej sieci LAN poprzez kabel.
2. W przypadku konieczności podłączenia do sieci WiFi (Ze względów bezpieczeństwa konieczne jest włączenie szyfrowania WEP/WPA - zalecane WPA2/WPA3. Zalecane jest Wyłączenie funkcji WPS oraz Zmniejszenie zasięgu **sieci WFI.**) . Zabronione jest korzystanie z zewnętrznych, sieci WiFi, na przykład WiFi hotelowe, w galeriach handlowych lub hot-spot w kawiarniach.

Dostęp do panelu konfiguracyjnego urządzenia sieciowego (routera) oraz dostęp do sieci bezprzewodowej (sieci WiFi) powinien być zabezpieczony silnym hasłem, którym nie jest hasło domyślne, zdefiniowane podczas pierwszej konfiguracji urządzenia.

Oprogramowanie urządzenia sieciowego powinno być regularnie aktualizowane.

Możliwość konfiguracji sprzętu sieciowego z urządzeniami znajdującymi się poza siecią LAN powinna być wyłączona lub ograniczona tylko do zdefiniowanych adresów IP.

§ 4

Procedura bezpiecznego logowania

Dostęp do sprzętu lub programu wykorzystywanego do pracy zdalnej powinien być możliwy wyłącznie z wykorzystaniem indywidualnego identyfikatora oraz hasła.

Hasło do sprzętu lub programu wykorzystywanego do pracy zdalnej powinno być odpowiednio długie i złożone. Nie powinno być ono zbudowane za pomocą ciągu

znajdujących się obok siebie znaków na klawiaturze lub oparte na prostych skojarzeniach związanych z użytkownikiem, na przykład numer telefonu, data urodzenia, imiona lub nazwiska.

Zabronione jest udostępnianie osobom trzecim haseł oraz przechowywanie ich w miejscach nie gwarantujących ich poufności.

Zabronione jest domyślne zapamiętywanie hasła dostępu do konta użytkownika systemu na sprzęcie oraz programów wykorzystywanych w pracy zdalnej.

Każdy komputer wykorzystywany do pracy zdalnej powinien posiadać:

a) indywidualny identyfikator oraz silne hasło,

b) zainstalowany najnowszy system operacyjny lub jego poprzednią wersję stabilną wraz z aktualizacjami zabezpieczeń Windows Profesional 10/11, FortiClient EMS.

c) zainstalowany system antywirusowy (zalecany FortiClient EMS) na bieżąco aktualizowany.

d) ustawiony wygaszacz ekranu, który blokuje urządzenie na wypadek kilkuminutowej nieaktywności użytkownika.

Pracując w systemach informatycznych, do których logujemy się metodą uwierzytelniania wykorzystując login i hasło, należy pamiętać aby nie odchodzić od komputera pozostawiając system zalogowany. Każdorazowo należy się wylogować.

Nie powinno się w przypadku logowania do systemów lub poczty służbowej korzystać z funkcji zapamiętywania haseł.

Należy zadbać aby wszelkie oprogramowanie narzędziowe (np. Adobe Reader, Java etc.) były zawsze zainstalowane w najnowszej wersji. To samo dotyczy się używanych przeglądarek, z których następuje logowanie do systemów informatycznych.

Jeżeli komputer, który wykorzystujemy do czynności służbowych jest i musi być współdzielony z innymi osobami (np. pozostali członkowie rodziny) należy w tym przypadku założyć osobny profil logowania do systemu zabezpieczony hasłem (np. w systemie Windows otrzymujemy swój własny pulpit, odrębny obszar na dysku roboczym) – w przypadku wykorzystania innego komputera niż służbowy.

Wszelkie dane przetwarzane na komputerze związane z naszą pracą w formie plików w postaci elektronicznej (excel, word, pdf) jeśli już nie są wykorzystywane powinny być usuwane z komputera w sposób trwały (wyrzucenie pliku do kosza nie jest jego usunięciem w sposób trwały) uniemożliwiający w późniejszym czasie dostęp do nich.

W przypadku korzystania z poczty służbowej na innym komputerze niż służbowy, należy pamiętać aby przysyłając wszelkie dane finansowe, osobowe etc. należy je zabezpieczyć poprzez wcześniejsze zaszyfrowanie z wykorzystaniem np. programów typu WinRAR, ZIP, które umożliwiają archiwizację plików wraz z zabezpieczeniem ich hasłem

W przypadku jeśli użytkownik komputera zauważy jakiegokolwiek niewłaściwe „zachowanie”, dziwne i niestandardowe działanie komputera, należy w pierwszej kolejności zaprzestać jakiegokolwiek pracy z tym komputerem w sposób natychmiastowy kończąc jego pracę (nawet poprzez bezpośrednie wyciągnięcie wtyczki zasilania), a następnie poinformować Administratora Danych Osobowych o zaistniałym fakcie.

§ 5

Bezpieczne korzystanie z programów i platform wykorzystywanych w pracy zdalnej (w tym wideokonferencji)

1) Użycie w pracy zdalnej danego programu/platformy wymaga pisemnej zgody pracodawcy.

1. Przed rozpoczęciem korzystania z programu/platformy wykorzystywanej do pracy zdalnej pracownik zobowiązany jest do zapoznania się z ogólnymi warunkami jej użytkowania oraz polityką prywatności.

2. W przypadku korzystania z programów z funkcją wideokonferencji zaleca się wyłączenie opcji nagrywania i przechowywania.

3. Przy podłączaniu się do programu z funkcją telekonferencji zalecane jest korzystanie z kodów dostępu/PIN-ów.

4. Przed rozpoczęciem korzystania z programów z funkcją telekonferencji zalecane jest przeskanowanie ich systemem antywirusowym lub *Anti-Malwarem*.

5. W trakcie korzystania z programów lub platform do pracy zdalnej należy ograniczyć ilość podawanych danych osobowych (zasada minimalizacji danych).

6. W przypadku kiedy pracownikowi został przydzielony służbowy adres e-mail zabronione jest korzystanie z prywatnego adresu e-mail do celów służbowych.

7. Zabrania się udostępniania dokumentów służbowych, za pomocą publicznego czatu lub innych komunikatorów.

8. Zabrania się udostępniania w mediach społecznościowych linków do konferencji, prowadzonych zajęć i innych aktywności realizowanych w ramach pracy zdalnej.

9. Należy korzystać z opcji „poczekalnia” tak, aby kontrolować uczestników telekonferencji, w celu uniknięcia przypadkowych lub niechcianych osób.

§ 6

Bezpieczne przechowywanie danych

Sprzęt komputerowy i inne nośniki urządzeń mobilnych wykorzystywane w celach służbowych, w tym laptop, telefon lub tablet powinny być zaszyfrowane, na przykład za pomocą hasła i zabezpieczone przed dostępem osób trzecich.

Zewnętrzne karty pamięci, a także inne nośniki danych, takie jak pendrive lub dysk zewnętrzny, wykorzystywane w celach służbowych powinny być szyfrowane, na przykład za pomocą hasła i zabezpieczone przed dostępem osób trzecich.

Zabronione jest umieszczanie danych osobowych w publicznych chmurach obliczeniowych (np. Dysk Google), komunikatorach (np. Messenger lub Discord) lub innych usługach dostępnych w sieci oraz rekomendowanie zakładania tam kont.

§ 7

Ochrona przed cyberatakami

Sprzęt wykorzystywany do pracy zdalnej musi być wyposażony w uruchomione i zaktualizowane oprogramowanie antywirusowe.

Systemy, w tym system operacyjny wykorzystywany do pracy zdalnej musi być regularnie aktualizowany.

Komputer wykorzystywany do pracy zdalnej musi mieć uruchomioną zaporę sieciową.

§ 8

Procedury bezpieczeństwa podczas pracy zdalnej

Zabrania się samodzielnej lub z wykorzystaniem wsparcia podmiotów zewnętrznych naprawy sprzętu służbowego wykorzystywanego do pracy zdalnej. W celu naprawy uszkodzonego sprzętu służbowego należy bezzwłocznie zwrócić go pracodawcy.

Zabrania się drukowania dokumentów służbowych w punktach ksero lub z pomocą innych podmiotów czy osób trzecich.

Pracownik zobowiązany jest do weryfikowania nadawców wiadomości e-mail. W przypadku wątpliwości co do tożsamości nadawcy zabronione jest otwieranie załączników do wiadomości e-mail oraz hiperłączy znajdujących się w tekście.

Podczas wysyłania korespondencji zbiorczej pracownik zobowiązany jest do korzystania z opcji „kopia ukryta” (pole UDW– Ukryci Do Wiadomości lub BCC– Blind Carbon Copy), dzięki której odbiorcy wiadomości nie zobaczą wzajemnie swoich adresów e-mail.

Pracownik zobowiązany jest do szyfrowania wiadomości e-mailowych zawierających dane osobowe i przekazywania hasła zawsze inną formą, na przykład telefonicznie.

Zabronione jest przesyłanie służbowych wiadomości e-mail na prywatne konta e-mail.

Zabrania się włączać opcję autouzupełniania formularzy w opcjach przeglądarki internetowej.

W przypadku korzystania z przeglądarki internetowej należy sprawdzić informacje o jej zabezpieczeniach. W tym celu należy kliknąć na symbol stanu bezpieczeństwa na lewo od adresu internetowego( Bezpieczna,  Informacje lub  Niezabezpieczona,  Niezabezpieczona lub Niebezpieczna), gdzie wyświetli się informacja o stopniu prywatności połączenia.

§ 9

Dodatkowe zalecenia do pracy zdalnej na prywatnym sprzęcie komputerowym

Pracownik zobowiązany jest do stworzenia oddzielnego konta użytkownika systemu w pracy na prywatnym sprzęcie komputerowym, wykorzystywanym do pracy zdalnej. Konto użytkownika powinno posiadać ograniczone uprawnienia i być chronione silnym hasłem oraz nieudostępniane osobom trzecim.

Za legalność oprogramowania, w tym programu antywirusowego odpowiada właściciel sprzętu.

Po zakończeniu okresu pracy poza miejscem jej stałego wykonywania pracownik jest zobowiązany bezzwłocznie przekazać pracodawcy wszystkie dane związane z wykonywanymi zadaniami służbowymi zapisane na prywatnym sprzęcie (dokumenty służbowe tworzone i przechowywane w pamięci komputera, pliki oraz inne posiadane informacje), a następnie usunąć je w sposób trwały.

§ 10

Bezpieczne przetwarzanie danych osobowych zawartych w dokumentacji papierowej podczas pracy zdalnej

Dokumentacja papierowa zawierająca dane osobowe udostępniana jest pracownikowi w zakresie niezbędnym do realizacji obowiązków służbowych podczas pracy zdalnej, za pisemną zgodą pracodawcy.

Po otrzymaniu zgody na piśmie pracownik sporządza kopie dokumentów niezbędnych do realizacji jego obowiązków służbowych podczas pracy zdalnej.

Zabronione jest zabieranie poza siedzibę pracodawcy oryginałów dokumentów.

Po wykonaniu kopii dokumentów pracownik przygotowuje zestawienie określające jakie dokumenty, w jakiej liczbie zostały skopiowane, następnie przekazuje je pracodawcy.

Pracodawca prowadzi ewidencje wydanych pracownikom dokumentów zawierających dane osobowe.

Podczas przenoszenia dokumentów pracownik zobowiązany jest do odpowiedniego ich zabezpieczenia i przenoszenia w taki sposób, aby były niewidoczne dla osób trzecich, na przykład w teczce wykonanej z nieprzezroczystego materiału.

Praca z dokumentami nie może być wykonywana w miejscach publicznych, na przykład w kawiarni, galerii handlowej itp.

Podczas pracy zdalnej pracownik zobowiązany jest przechowywać udostępnione kopie dokumentów papierowych tylko przez okres niezbędny do wykonania określonego zadania podczas pracy zdalnej (zasada ograniczenia przetwarzania). Po tym czasie zobowiązany jest niezwłocznie zwrócić je pracodawcy.

Po weryfikacji kompletności dokumentów zwróconych przez pracownika, pracodawca brakuje je zgodnie z obowiązującymi przepisami prawa.

Zabrania się pracownikowi samodzielnego niszczenia dokumentacji uzyskanej od pracodawcy lub samodzielnie wytworzonej.

Pracownik zobowiązany jest zabezpieczyć posiadaną dokumentację i po zakończeniu pracy zdalnej niezwłocznie zwrócić ją do pracodawcy.

§ 11

Naruszenie ochrony danych osobowych podczas pracy zdalnej

Pracownik, który stwierdzi lub podejrzewa naruszenie ochrony danych osobowych w systemie informatycznym lub w systemie tradycyjnym, zobowiązany jest do niezwłocznego pisemnego poinformowania o tym pracodawcę – administratora danych (załącznik nr 1).

W przypadku powzięcia informacji o naruszeniu ochrony danych osobowych Administrator danych prowadzi postępowanie wyjaśniające podczas, którego:

- ustala zakres i przyczyny naruszenia ochrony danych osobowych oraz jego ewentualne skutki;

- informuje i konsultuje tok postępowania z Inspektorem Ochrony Danych;

- podejmuje działania prewencyjne zmierzające do eliminacji podobnych incydentów w przyszłości lub zmniejszenia strat w momencie ich zaistnienia.

Zgłoszenie naruszenia ochrony danych osobowych

1) Imię i nazwisko osoby zgłaszającej:

.....

1. Data i czas zaistnienia/ rozpoczęcia naruszenia

.....

2. Naruszenie ochrony danych dotyczyło:

1) zgubienia lub kradzieży nośnika/urządzenia;

- dokumentacja papierowa (zawierająca dane osobowe) zgubiona, skradziona lub pozostawiona w niebezpiecznej lokalizacji;
- korespondencja papierowa utracona przez operatora pocztowego lub otwarta przed zwróceniem nadawcy;
- nieuprawnione uzyskanie dostępu do informacji;
- nieuprawnione uzyskanie dostępu do informacji poprzez złamanie zabezpieczeń;
- złośliwe oprogramowanie ingerujące w poufność, integralność i dostępność danych;
- uzyskanie poufnych informacji poprzez pozornie zaufaną osobę w oficjalnej komunikacji elektronicznej;
- nieprawidłowa anonimizacja danych osobowych w dokumencie;
- nieprawidłowe usunięcie/ zniszczenie danych osobowych z nośnika/ urządzenia elektronicznego przed jego zbyciem przez administratora;
- niezamierzona publikacja;
- dane osobowe wysłane do niewłaściwego odbiorcy;
- ujawnienie danych niewłaściwej osobie;
- ustne ujawnienia danych osobowych;
- inne:

3. Szczegółowy opis kategorii osób (np. uczniów) i danych osobowych (np.: imię, nazwisko, data urodzenia, miejsce zamieszkanie, dane dotyczące zdrowia):

.....
.....

4. Opis okoliczności naruszenia

.....
.....
.....
.....
.....