Zarządzenie Nr OR.120.25.2023
Starosty Kluczborskiego
z dnia 16 maja 2023 r.

w sprawie ustalenia Regulaminu pracy zdalnej oraz Procedury ochrony informacji oraz danych osobowych podczas pracy zdalnej w Starostwie Powiatowym w Kluczborku

Na podstawie art. 67^{20} §4 oraz art. 67^{26} §1 ustawy z dnia 26 czerwca 1974 r. – Kodeks pracy (Dz.U. z 2022 r. poz. 1510 z późn.zm.), art. 35 ust. 2 ustawy z dnia 5 czerwca 1998 r. o samorządzie powiatowym (Dz. U. z 2022 r., poz. 1526 z późn zm.) oraz § 15 ust. 3 pkt. 2 lit. a Regulaminu Organizacyjnego Starostwa Powiatowego w Kluczborku przyjętego Uchwałą Nr 193/762/2023 Zarządu Powiatu w Kluczborku z dnia 31 stycznia 2023 r. w sprawie uchwalenia Regulaminu Organizacyjnego Starostwa Powiatowego w Kluczborku, zarządza się, co następuje:

§ 1. Ustala się Regulamin pracy zdalnej w Starostwie Powiatowym w Kluczborku stanowiący załącznik nr 1 do niniejszego zarządzenia oraz Procedurę ochrony informacji oraz danych osobowych podczas pracy zdalnej stanowiącą załącznik nr 2 do niniejszego zarządzenia.

§ 2. Zarządzenie wchodzi w życie z dniem podjęcia.

STAROSTA
Mirosław Birecki

Radca Prawny
Dariusz Kraśnicki
16.05.2023 r.

Załącznik Nr 1
do Zarządzenia Nr OR.120.25.2023
Starosty Kluczborskiego z dnia 16.05.2023 r.

Regulamin pracy zdalnej w Starostwie Powiatowym w Kluczborku

I Postanowienia ogólne

§1. 1. Regulamin pracy zdalnej, zwany dalej Regulaminem określa zasady wykonywania pracy zdalnej oraz związane z tym prawa i obowiązki Pracodawcy i Pracowników Starostwa Powiatowego w Kluczborku.
2. Ilekroć w Regulaminie jest mowa o:
1) Pracodawcy – rozumie się przez to Starostwo Powiatowe w Kluczborku;
2) Pracowniku – rozumie się przez to osoby zatrudnione na postawie stosunku pracy u Pracodawcy, bez względu na rodzaj stosunku pracy oraz wymiar czasu pracy;
3) Starostwie – rozumie się przez to Starostwo Powiatowe w Kluczborku;
4) Informatyku – rozumie się przez to pracownika zatrudnionego w Wydziale Organizacyjnym zajmującym się obsługą oraz zarządzaniem systemem informatycznym w Starostwie;
5) Pracy zdalnej - rozumie się przez to pracę wykonywaną całkowicie lub częściowo w miejscu wskazanym przez Pracownika i każdorazowo uzgodnionym z Pracodawcą, w tym pod adresem zamieszkania Pracownika, w szczególności przy wykorzystaniu środków bezpośredniego porozumiewania się na odległość;
6) Kodeks pracy – rozumie się przez to ustawę z dnia 26 czerwca 1974 r. Kodeks pracy.

§2. Pracą zdalną mogą być objęci pracownicy wykonujący pracę administracyjno – biurową niezwiązaną z bezpośrednią obsługą klientów oraz której świadczenie jest możliwe przy wykorzystaniu środków bezpośredniego porozumiewania się na odległość.

§3. Uzgodnienie między Pracodawcą, a Pracownikiem dotyczące wykonywania pracy w trybie zdalnym w trakcie trwania zatrudnienia może być dokonane z inicjatywy Pracodawcy lub na pisemny wniosek Pracownika złożony w formie papierowej lub elektronicznej.

§4. 1. Praca zdalna może być wykonywana na polecenie Pracodawcy, w sytuacjach określonych w art. 67^{19} §3 Kodeksu pracy.
2. Pracodawca może w każdym czasie cofnąć polecenie wykonywania pracy zdalnej, o którym mowa w ust. 1, z co najmniej dwudniowym uprzedzeniem.
3. W przypadku zmiany warunków lokalowych i technicznych uniemożliwiającej wykonywanie pracy zdalnej Pracownik informuje o tym niezwłocznie Pracodawcę. W takim przypadku Pracodawca niezwłocznie cofa polecenie wykonywania pracy zdalnej.
4. Polecenie wydawane jest każdorazowo na czas określony, nie dłuższy niż 1 miesiąc, z możliwością jego przedłużenia.

II Obowiązki Pracodawcy i Pracownika wykonującego pracę zdalną

§5. 1. Za właściwe organizowanie procesu pracy, z uwzględnieniem realizacji bieżących zadań oraz obowiązujących norm czasu pracy Pracownika wykonującego pracę zdalną odpowiada jego bezpośredni przełożony.
2. Pracownik wykonujący pracę zdalną jest zobowiązany do:
1) bieżącego wykonywania zadań wynikających z jego zakresu czynności oraz zadań zleconych przez bezpośredniego przełożonego;
2) pozostawania w stałej gotowości do świadczenia pracy w godzinach pracy zgodnych z rozkładem czasu pracy Pracownika, w szczególności dostępności telefonicznej oraz e-mailowej;
3) pozostawania w stałym kontakcie ze współpracownikami oraz przełożonymi;

4) potwierdzania obecności w pracy poprzez zalogowanie się do systemu operacyjnego w godzinie rozpoczęcia pracy oraz kontakt e-mailowy z bezpośrednim przełożonym;
5) dbania o powierzony sprzęt do wykonywania pracy zdalnej oraz wykorzystywania go wyłącznie dla celów służbowych;
6) stosowania obowiązujących w Starostwie procedur ochrony informacji oraz danych osobowych podczas pracy zdalnej oraz innych obowiązujących wymogów w zakresie bezpieczeństwa i ochrony informacji;
7) zorganizowania swojego stanowiska pracy w sposób zapewniający bezpieczne i higieniczne warunki pracy.

§6. 1. Pracownik może być dopuszczony do wykonywania pacy zdalnej wyłącznie w przypadku złożenia przez Pracownika oświadczenia w postaci papierowej lub elektronicznej, zawierającego potwierdzenie, że na stanowisku pracy zdalnej w miejscu wskazanym przez pracownika i uzgodnionym z pracodawcą są zapewnione bezpieczne i higieniczne warunki tej pracy.
2. Przed dopuszczeniem do wykonywania pracy zdalnej pracownik potwierdza w oświadczeniu składanym w postaci papierowej lub elektronicznie zapoznanie się z oceną ryzyka zawodowego uwzględniającą wpływ pracy zdalnej na wzrok, układ mięśniowo – szkieletowy oraz uwarunkowania psychospołeczne tej pracy oraz z informacją, o której mowa w art. 67^{31} § 5 oraz zobowiązuje się do ich przestrzegania.

§7. 1. Pracownik jest zobowiązany do zapoznania się z zasadami bezpieczeństwa i ochrony informacji oraz procedurą ochrony informacji oraz danych osobowych podczas pracy zdalnej obowiązującymi w Starostwie.
2. Pracownik potwierdza zapoznanie się z zasadami i procedurami, o których mowa w ust. 1 podpisując oświadczenie i zobowiązuje się do ich przestrzegania.

§8. W okresie wykonywania pracy zdalnej Pracownik ma obowiązek stawić się w siedzibie Pracodawcy na każde wezwanie Pracodawcy w godzinach zgodnych ze swoim rozkładem czasu pracy.

III Narzędzia pracy oraz koszty pracy zdalnej

§9. 1. W celu wykonywania pracy Pracownik wykorzystuje sprzęt przekazany przez Pracodawcę potwierdzając jego otrzymanie własnoręcznym podpisem w rejestrze wypożyczenia sprzętu komputerowego do pracy zdalnej.
2. W indywidualnych przypadkach pomiędzy Pracownikiem, a Pracodawcą może zostać zawarta umowa użyczenia sprzętu w celu wykonywania pracy zdalnej.
3. Pracownik odpowiada za bezpieczne przechowywanie sprzętu oraz brak dostępu osób trzecich do jakichkolwiek informacji znajdujących się na sprzęcie komputerowym.
4. Pracodawca zapewnia Pracownikowi niezbędne wsparcie techniczne w trakcie pracy, a Pracownik jest zobowiązany zgłaszać wszelkie potrzeby w tym zakresie poprzez kontakt e-mailowy lub telefoniczny z Informatykami.
5. Pracownik może korzystać ze zdalnej pomocy Informatyków Starostwa, w celu rozwiązania bieżących problemów technicznych.
6. W celu serwisu sprzętu oraz instalacji i aktualizacji oprogramowania Pracownik jest zobowiązany stawić się w siedzibie Pracodawcy w terminie umówionym z bezpośrednim przełożonym oraz Informatykami.

§10. 1. Pracownik wykonując pracę zdalną może wykorzystywać własny sprzęt komputerowy spełniający wymagania techniczne i zabezpieczenia umożliwiające udostępnienie zdalnego dostępu do komputera służbowego, obsługę poczty elektronicznej oraz aplikacji niezbędnych do świadczenia pracy na danym stanowisku pracy.
2. Szczegółowe wymagania dotyczące wykorzystywania własnego sprzętu przez Pracownika zostały określone w Procedurze ochrony informacji oraz danych osobowych podczas pracy zdalnej.
3. Oceny spełnienia wymagań, o których mowa w ust. 1 i 2 dokonują Informatycy.
4. Pracownikowi korzystającemu z własnego sprzętu podczas pracy zdalnej Pracodawca udostępnia zdalny dostęp do komputera służbowego (zdalny pulpit), jeżeli istnieje taka możliwość i potrzeba oraz dostęp do służbowej skrzynki e-mailowej.

§11. 1. W celu pokrycia Pracownikowi kosztów związanych z wykonywaniem pracy zdalnej, tj. kosztów energii elektrycznej, usług telekomunikacyjnych niezbędnych do wykonywania pracy zdalnej oraz kosztów związanych z używaniem własnego sprzętu przez Pracownika, Pracodawca wypłaca Pracownikowi ryczałt odpowiadający przewidywanym kosztom ponoszonym przez Pracownika w związku z pracą zdalną.
2. Kwota ryczałtu jest ustalana przez Starostę Kluczborskiego w drodze odrębnego zarządzenia w stosunku do Pracowników wykorzystujących sprzęt przekazany przez Pracodawcę oraz w stosunku do Pracowników wykorzystujących własny sprzęt do pracy zdalnej.
3. Wysokość ryczałtu jest proporcjonalna do wymiaru zatrudnienia pracownika.
4. Ryczałt nie przysługuje za dni nieobecności w pracy Pracownika świadczącego pracę zdalną. W przypadku pracy wykonywanej częściowo zdalnie ryczałt przysługuje za dni, w których pracownik świadczył pracę w trybie zdalnym.
5. Ryczałt wypłacany jest na rachunek osobisty pracownika do 15 - go dnia miesiąca następującego po miesiącu, w którym Pracownik wykonywał pracę zdalną.
6. Ryczałt wypłaca się na podstawie wykazu obecności w pracy sporządzonego przez pracownika na Samodzielnym Stanowisku ds. Personalnych odrębnie dla każdego pracownika uprawnionego do otrzymania ryczałtu.

IV Zasady kontroli Pracownika wykonującego pracę zdalną

§12. Pracodawca w każdym czasie, w godzinach pracy Pracownika, może sprawdzić wykonywanie przez niego pracy wykorzystując w tym celu dostępne narzędzia teleinformatyczne lub/i telefon.

§13. 1. Pracodawca może przeprowadzić kontrolę pracy zdalnej u Pracownika w ustalonym miejscu jej świadczenia w godzinach zgodnych z rozkładem czasu pracy Pracownika.
2. Kontrola może dotyczyć wykonywania pracy zdalnej, bezpieczeństwa i higieny pracy oraz przestrzegania wymogów w zakresie bezpieczeństwa i ochrony informacji, w tym procedury ochrony informacji oraz danych osobowych podczas pracy zdalnej.
3. Kontroli w zakresie, o którym mowa w ust. 2 dokonuje upoważniony Pracownik Starostwa.

§14. 1. Kontrola odbywa się w obecności Pracownika w uzgodnionym z nim dniu.
2. Pracownik upoważniony do przeprowadzenia kontroli na co najmniej 3 dni przed jej datą przekazuje drogą e-mailową Pracownikowi wykonującemu pracę zdalną informację o kontroli i jej zakresie.
3. Wykonywanie czynności kontrolnych nie może naruszać prywatności Pracownika wykonującego pracę zdalną i innych osób ani utrudniać korzystania z pomieszczeń domowych w sposób zgodny z ich przeznaczeniem.

§15. 1. Kontrolujący z przeprowadzonej kontroli sporządza protokół.
2. Jeżeli w wyniku kontroli zostaną stwierdzone uchybienia w przestrzeganiu przepisów i zasad w zakresie bezpieczeństwa i higieny pracy lub w przestrzeganiu wymogów w zakresie bezpieczeństwa i ochrony informacji, w tym procedur ochrony informacji oraz danych osobowych podczas pracy zdalnej Pracodawca zobowiązuje Pracownika do usunięcia stwierdzonych uchybień w terminie wskazanym w zaleceniach pokontrolnych.
3. W przypadku stwierdzonych uchybień Pracodawca może także cofnąć zgodę na wykonywanie pracy zdalnej przez tego Pracownika określając termin rozpoczęcia pracy w dotychczasowym miejscu pracy (stacjonarnie).

V Praca zdalna wykonywana okazjonalnie

§17. Praca zdalna może być wykonywana okazjonalnie, na wniosek Pracownika złożony w postaci papierowej lub elektronicznej, w wymiarze nieprzekraczającym 24 dni w roku kalendarzowym.

§18. 1. Pracownik składa wniosek o pracę zdalną wykonywaną okazjonalnie na co najmniej 3 dni przed terminem jej rozpoczęcia w celu uzyskania zgody Pracodawcy.
2. Wniosek, o którym mowa w ust. 1 wymaga akceptacji bezpośredniego przełożonego.

3. Pracodawca wyraża zgodę bądź nie wyraża zgody na pracę zdalną wykonywaną okazjonalnie poprzez dekretację na wniosku Pracownika, po uzyskaniu informacji o możliwości udostępnienia sprzętu służbowego do pracy zdalnej lub po dokonaniu oceny spełnienia wymagań dotyczących wykorzystania prywatnego sprzętu do wykonywania pracy zdalnej, o której mowa w §10 ust. 3 przez Informatyków.
4. W przypadku zgody Pracodawcy Pracownik na Samodzielnym Stanowisku ds. Personalnych przekazuje niezwłocznie Informatykom drogą e-mailową informację o wykonywaniu oraz okresie wykonywania przez Pracownika pracy zdalnej.
5. Po uzyskaniu zgody Pracodawcy Pracownik niezwłocznie kontaktuje się z Informatykami, w celu uzyskania niezbędnych dostępów umożliwiających pracę zdalną.

§19. 1. Pracownik nie może rozpocząć pracy zdalnej bez pisemnej zgody Pracodawcy.
2. Pracownik nie może rozpocząć pracy zdalnej bez złożenia oświadczeń wynikających z §6, §7 oraz §23 niniejszego Regulaminu.

§20. Pracownik na Samodzielnym Stanowiska ds. Personalnych zaznacza na liście obecności fakt wykonywania przez Pracownika pracy zdalnej w danym dniu.

§21. Do pracy zdalnej wykonywanej okazjonalnie nie mają zastosowania zapisy §11 niniejszego Regulaminu.

VI Postanowienia końcowe

§22. Wzory wniosków oraz oświadczeń wynikających z niniejszego Regulaminu są dostępne dla Pracowników w Intranecie oraz na Samodzielnym Stanowisku ds. Personalnych.

§23. Przed rozpoczęciem wykonywania pracy w trybie zdalnym Pracownik zobowiązany jest do zapoznania się z niniejszym Regulaminem oraz zobowiązuje się do jego stosowania podpisując stosowne oświadczenie.

§24. Podczas pracy zdalnej Pracownik jest zobowiązany do przestrzegania obowiązków i postanowień wynikających z regulacji wewnątrzzakładowych obowiązujących w Starostwie Powiatowym w Kluczborku oraz przepisów powszechnie obowiązujących.

STAROSTA
Mirosław Birecki

Niniejszy Regulamin pracy zdalnej w Starostwie Powiatowym w Kluczborku skonsultowano z przedstawicielami pracowników:

Dorota Jaworska
(podpis przedstawiciela pracowników)

Andrzej Duraj
(podpis przedstawiciela pracowników)

Załącznik Nr 2
do Zarządzenia Nr OR.120.25.2023
Starosty Kluczborskiego z dnia 16.05.2023 r.

Procedura ochrony informacji oraz danych osobowych podczas pracy zdalnej

I Zakres oraz cel procedury

§1. 1. Procedura ochrony informacji oraz danych osobowych podczas pracy zdalnej, zwana dalej „Procedurą" określa zasady postępowania z informacjami oraz danymi osobowymi, stosowanie zabezpieczeń i ochrony podczas wykonywania pracy zdalnej.

2. Obowiązek stosowania Procedury dotyczy wszystkich pracowników wykonujących pracę zdalną bez względu na tryb w jakim pracownik wykonuje pracę zdalną.

II Definicje

§2. Ilekroć w procedurze jest mowa o:

1) Pracodawcy – rozumie się przez to Starostwo Powiatowe w Kluczborku;
2) Administratorze danych – rozumie się przez to Starostę Kluczborskiego;
3) Pracowniku – rozumie się przez to osoby zatrudnione na podstawie stosunku pracy u Pracodawcy, bez względu na rodzaj stosunku pracy oraz wymiar czasu pracy;
4) Informatyku – rozumie się przez to pracownika zatrudnionego w Wydziale Organizacyjnym zajmującym się obsługą oraz zarządzaniem systemem informatycznym w Starostwie;
5) Pracy na sprzęcie służbowym – rozumie się przez to narzędzia oraz sprzęt udostępniony przez Pracodawcę pracownikowi wykonującemu prace zdalną;
6) Pracy na sprzęcie prywatnym – rozumie się przez to prywatny sprzęt komputerowy pracownika, używany w celu wykonywania pracy zdalnej;
7) Bezpieczeństwie informacji – rozumie się przez to zapewnienie poufności, integralności i dostępności przetwarzanych danych osobowych;
8) Pracy zdalnej - rozumie się przez to pracę wykonywaną całkowicie lub częściowo w miejscu wskazanym przez Pracownika i każdorazowo uzgodnionym z Pracodawcą, w tym pod adresem zamieszkania Pracownika, w szczególności przy wykorzystaniu środków bezpośredniego porozumiewania się na odległość;
9) IOD – należy przez to rozumieć Inspektora Ochrony Danych powoływanego przez Administratora zgodnie z RODO;
10) RODO – należy przez to rozumieć rozporządzenie Parlamentu Europejskiego (UE) 2016/679 z 27 kwietnia 2016r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE wraz ze zmianami.

III Dokumentacja ochrony danych

§3. 1. Dokumentację ochrony informacji oraz danych osobowych u Pracodawcy stanowi:

1) Polityka ochrony danych osobowych;
2) Polityka przetwarzania danych osobowych;
3) Polityka bezpieczeństwa systemów informatycznych;
4) Instrukcja zarządzania systemem informatycznym;
5) Procedura ochrony informacji i danych osobowych podczas pracy zdalnej.

2. Pracownik jest zobowiązany do przestrzegania oraz stosowania zasad ochrony informacji i danych osobowych, w tym zasad uzyskiwania dostępu, przesyłania, przechowywania danych oraz wykonywania obowiązków związanych z przetwarzaniem danych osobowych.

IV Przygotowanie narzędzi oraz sprzętu

§4. 1. Pracownik do wykonywania pracy zdalnej może otrzymać sprzęt służbowy, przygotowany oraz udostępniony przez Pracodawcę do pracy zdalnej, powyższy fakt przekazania sprzętu zostaje odnotowany w prowadzonym rejestrze wypożyczenia sprzętu komputerowego do pracy zdalnej, poprzez własnoręczny podpis.

2. Pracownik po skończeniu pracy zdalnej zwraca do Informatyków sprzęt udostępniony przez Pracodawcę, a powyższy fakt zostaje odnotowany w rejestrze wypożyczenia sprzętu komputerowego do pracy zdalnej.

3. W przypadku braku dostępnego sprzętu oraz narzędzi do wykonywania pracy zdalnej przez Pracownika podczas wykonywania pracy zdalnej dopuszcza się wykorzystanie prywatnego sprzętu Pracownika po spełnieniu minimalnych wymagań dotyczących oprogramowania oraz sprzętu niezbędnego do bezpiecznej pracy zdalnej.

V Praca na własnym sprzęcie komputerowym

§5. 1. Aby wykonywać pracę zdalną na prywatnym sprzęcie stanowiącym własność Pracownika, sprzęt musi spełnić minimalne wymagania dotyczące bezpieczeństwa podczas przetwarzania danych osobowych.

2. W celu dopuszczenia prywatnego sprzętu do pracy zdalnej, przed rozpoczęciem pracy, sprzęt musi zostać sprawdzony pod kątem spełnienia wymagań, o których mowa w ust. 1 przez Informatyków w Wydziale Organizacyjnym.
Sprawdzenie sprzętu prywatnego jest obowiązkowe i przeprowadzane każdorazowo przed wydaniem przez Pracodawcę zgody na pracę zdalną przy wykorzystaniu sprzętu prywatnego.

3. Ocena spełnienia wymagań może się odbyć poprzez dostarczenie sprzętu prywatnego przez Pracownika do siedziby Starostwa (sprzęt przenośny) lub zdalnie w przypadku posiadania komputera stacjonarnego.

4. Minimalne wymagania w zakresie bezpieczeństwa sprzętu prywatnego są następujące:

1) na urządzeniu musi być zainstalowane legalne i aktualnie wspierane oprogramowanie oraz system operacyjny;
2) na urządzeniu musi być zainstalowane aktualne i licencjonowane oprogramowanie antywirusowe wraz z firewallem działające w tle;
3) zapora z oprogramowania antywirusowego musi być włączona;
4) zalogowanie do systemu operacyjnego wymaga uwierzytelnienia poprzez podanie indywidualnego loginu i hasła użytkownika, kodu PIN lub tokenu;
5) przeglądarka internetowa musi być ustawiona w taki sposób, aby nie było aktywne autouzupełnianie i zapamiętywanie hasła do strony lub portalu udostępnionego przez Pracodawcę do pracy zdalnej;
6) został zainstalowany program umożliwiający zaszyfrowanie i odszyfrowanie danych (np.: 7-Zip);
7) zostało ustawione automatyczne blokowanie dostępu do urządzenia po dłuższym braku aktywności;
8) dopuszczalne jest korzystanie z domowej sieci WIFI, pod warunkiem, że Pracownik ma odpowiednio zabezpieczoną sieć poprzez ustawienie hasła dostępu do swojej sieci WIFI.

5. Porad i wsparcia w zakresie konfiguracji sieci domowej, w tym jej zabezpieczenia na potrzeby pracy zdalnej, udzielają Informatycy Starostwa.

6. Pracodawca może dodatkowo wymagać, aby urządzenie wykorzystywane do pracy zdalnej zawierało inne zabezpieczenia takie jak:

1) zaszyfrowany dysk;
2) oprogramowanie służące do monitorowania wykonywania pracy przez Pracownika, wymaganymi zgodnie z przepisami prawa pracy.

VI Praca na sprzęcie służbowym

§6. 1. Pracownik po otrzymaniu sprzętu komputerowego od Pracodawcy musi przestrzegać zasad dotyczących wykorzystywania sprzętu służbowego oraz zabezpieczenia sprzętu, a mianowicie:

1) zabrania się instalowania jakiegokolwiek oprogramowania na sprzęcie służbowym bez zgody Informatyków Starostwa;
2) na sprzęcie służbowym nie może być instalowane żadne nielegalne oprogramowanie;
3) pracownik odpowiada za zabezpieczenie sprzętu służbowego przed dostępem osób trzecich, a w szczególności domowników i dzieci;
4) zabronione jest podłączanie nośników pamięci innych niż udostępnione przez Pracodawcę;
5) pracownik odpowiada za ochronę powierzonego sprzętu, nie może go uruchamiać oraz korzystać w miejscach publicznych;
6) podczas podłączenia sprzętu służbowego do swojej sieci WIFI, Pracownik musi mieć odpowiednio zabezpieczoną sieć, poprzez ustawienie hasła dostępu do swojej sieci WIFI;
7) pracownik nie może podłączać służbowego sprzętu do sieci niezabezpieczonych WIFI oraz do hot spotów publicznych;
8) laptop służbowy jest zabezpieczony hasłem, a w razie potrzeby jest szyfrowany również dysk;
9) zabronione jest ingerowanie w zabezpieczenia zainstalowane na urządzeniach służbowych;
10) zabrania się podłączania drukarek lub innych urządzeń oraz wykonywania skanów do wypożyczonego sprzętu służbowego, bez poinformowania i uzyskania zgody od Informatyków w Wydziale Organizacyjnym;
11) pracownik jest odpowiedzialny za zabezpieczenia danych podczas pracy zdalnej poprzez zapisywanie oraz szyfrowanie nośników zewnętrznych otrzymanych od Pracodawcy (pendrive itp.).

VII Dostęp do informacji i danych osobowych oraz praca z informacjami i danymi osobowymi

§7. 1. Pracownik w celu wykonywania pracy zdalnej uzyskuje dostęp do informacji i danych osobowych poprzez narzędzia oraz oprogramowanie udostępnione przez Pracodawcę. Dostęp do danych osobowych jest możliwy poprzez nadanie pracownikowi loginu i hasła do bezpiecznego połączenia, poprzez odpowiednią stronę internetową/portal (łączenie ze zdalnym pulpitem do komputera znajdującego się u Pracodawcy: dotyczy komputerów stacjonarnych w biurach w siedzibie Pracodawcy) lub poprzez specjalną aplikację łączącą się poprzez sieć VPN w przypadku wykorzystania przenośnego sprzętu służbowego.

2. Nie jest dopuszczalne wykorzystywanie informacji i danych osobowych przetwarzanych w ramach pracy zdalnej w innym celu niż wykonywanie obowiązków służbowych.

3. Pracownik utrzymuje w tajemnicy otrzymane od Informatyków dane dostępowe w celu zalogowania się do sieci firmowej VPN, w tym loginu i hasła oraz zabezpiecza je przed dostępem osób nieuprawnionych, w tym domowników.

4. Dane dostępowe do pracy zdalnej, czyli hasło jest zmieniane każdorazowo przez Informatyków w Wydziale Organizacyjnym, gdy Pracownik dostanie zgodę na pracę zdalną.

5. Pracownik jest zobowiązany do pracy w ramach przydzielonego mu loginu i hasła.

6. Zabrania się korzystania z konta, loginu i hasła innego Pracownika.

7. Dostęp do informacji i danych osobowych odbywa się w sposób zdalny i następuje poprzez:

1) dostęp do systemu informatycznego przetwarzającego informacje oraz dane osobowe poprzez pulpit zdalny;
2) dostęp do określonych zasobów w infrastrukturze Pracodawcy przy użyciu szyfrowanego połączenia zdalnego (np.: VPN);
3) dostęp do skrzynki pocztowej pracownika w domenie Pracodawcy.

8. Komunikacja służbowa odbywa się w sposób zapewniający bezpieczeństwo informacji i danych osobowych wyłącznie poprzez zabezpieczone połączenia.

9. Jeżeli Pracownik będzie musiał wysłać załączniki zawierające dane osobowe muszą one być zaszyfrowane odpowiednim oprogramowaniem (np.: 7-zip).

10. Nie należy przesyłać plików z danymi osobowymi (np.: w celu pracy z danymi osobowymi), jeżeli jest możliwy dostęp do danych w systemie informatycznym na sprzęcie w siedzibie Starostwa.

11. Drukowanie dokumentów na potrzeby wykonywania obowiązków służbowych należy ograniczyć do niezbędnego minimum.

12. Zabrania się Pracownikowi przesyłania służbowych wiadomości e-mail na prywatne konta e-mail.

13. W przypadku problemów technicznych w działaniu udostępnionego sprzętu służbowego lub oprogramowania należy niezwłocznie zgłosić problem do Informatyków.

VIII Przechowywanie danych osobowych i nośników

§8. 1. Pracownik odpowiada za bezpieczne przechowywanie danych osobowych, sprzętu oraz nośników służących do ich przetwarzania.

2. Sprzęt oraz nośniki zawierające dane osobowe nie powinny być pozostawione bez nadzoru. Po zakończeniu pracy sprzęt oraz nośniki i dokumentacja powinny być schowane w miejscu o utrudnionym dostępie, w celu zabezpieczenia przed osobami nieuprawnionymi.

3. Zabronione jest umieszczanie danych osobowych w publicznych chmurach obliczeniowych (np. dysk google itp.), komunikatorach np. Messenger itp.) lub innych usługach dostępnych w sieci.

IX Transport sprzętu i nośników danych

§9. 1. Pracownik odpowiada za bezpieczeństwo powierzonego mu sprzętu, nośników i dokumentacji podczas ich transportu, w szczególności zabrania się pozostawiania ich bez nadzoru (np. w środku transportu: samochodzie, komunikacji publicznej).

2. Przewożenie dokumentacji zawierającej dane osobowe powinno odbywać się w sposób zabezpieczony przed dostępem osób nieuprawnionych. W tym celu Pracownik umieszcza dokumentację w teczce lub skoroszycie uniemożliwiającym zapoznanie się z treścią danych osobowych, a następnie w plecaku lub torbie.

X Naruszenie ochrony informacji i danych osobowych podczas pracy zdalnej

§10. 1. Pracownik, który stwierdzi lub podejrzewa naruszenie informacji i danych osobowych w systemie informatycznym lub sprzęcie służbowym zobowiązany jest do natychmiastowego poinformowania Inspektora Ochrony Danych (IOD lub inną osobę wskazaną przez Pracodawcę).

2. W przypadku zauważenia nieprawidłowości w funkcjonowaniu systemów informatycznych lub sprzętu, na którym przetwarza informacje i dane osobowe, Pracownik podejmuje możliwe działania w celu zabezpieczenia danych podczas pracy zdalnej, a następnie powiadamia właściwe osoby zgodnie z ust. 1.

3. Pracownik jest zobowiązany zgłaszać w szczególności następujące incydenty:

1) naruszenie poufności, to jest ujawnienie informacji niepowołanym osobom;
2) naruszenie integralności, to jest zniszczenie, uszkodzenie lub przekłamanie informacji;

3) naruszenie dostępności, to jest braku dostępu do danych przez uprawnionych użytkowników;
4) niewłaściwe wykorzystanie zasobów informatycznych lub niewłaściwe postepowanie z dokumentacja papierową;
5) działania szkodliwego oprogramowania;
6) próby omijania systemów zabezpieczeń;
7) nieautoryzowany dostęp do systemów, aplikacji i dokumentów;
8) zniszczenie lub kradzież urządzeń wykorzystywanych do przetwarzania i przechowywania informacji;
9) zniszczenie lub kradzież nośników danych;
10) innych nieprawidłowości w zakresie zabezpieczenia przechowywania danych, w tym informacji i danych osobowych.

XI Stosowanie zabezpieczeń przez Pracowników przy pracy zdalnej

§11. Pracownik jest zobowiązany dbać o bezpieczeństwo informacji i danych osobowych przetwarzanych w ramach wykonywania obowiązków służbowych podczas pracy zdalnej. W tym celu, podczas codziennej pracy, Pracownik jest zobowiązany stosować poniższe zasady:

1) ogranicza do niezbędnego minimum drukowanie plików zawierających informacje i dane osobowe do sytuacji, gdy jest to konieczne;
2) niszczy robocze wydruki zawierające informacje i dane osobowe po ustaniu ich przydatności dla bieżącej pracy, zabrania się wyrzucać dokumenty zawierające informacje i dane osobowe do kosza, zniszczenie musi mieć charakter nieodwracalny np. przy użyciu niszczarki lub nożyczek;
3) cyklicznie usuwa niepotrzebne pliki zawierające dane osobowe, pobrane w celu pracy z nimi;
4) przechowuje dokumentację zawierającą dane osobowe w sposób bezpieczny, zamknięty w teczce, skoroszycie lub segregatorze w miejscu niedostępnym dla osób postronnych (w szafce, szafie);
5) wylogowuje się z systemów informatycznych i portali po zakończeniu pracy;
6) zabezpiecza ekran przed dostępem innych osób, w tym domowników, poprzez stosowanie wygaszaczy ekranów lub każdorazowo poprzez zablokowanie sprzętu przed odejściem od ekranu;
7) nie zapamiętuje oraz nie zapisuje w przeglądarkach internetowych danych dotyczących logowania do stron i portali wykorzystywanych w celu wykonywania pracy zdalnej ani innych systemów wykorzystywanych do pracy;
8) nie korzysta ani nie uruchamia programów i aplikacji pochodzących od nieznanych dostawców;
9) nie udostępnia domownikom sprzętu służbowego przeznaczonego do pracy zdalnej.

STAROSTA
Mirosław Birecki