Załącznik nr 2 do Regulaminu

Kwestionariusz analizy ryzyka pracy zdalnej

pracownika Urzędu Marszałkowskiego Województwa Kujawsko-Pomorskiego w Toruniu
przeprowadzonej na podstawie złożonego wniosku z dnia ……..

Imię i nazwisko pracownika ……
Departament ……
Wydział ……
Biuro ……..
Imię i nazwisko kierownika / osoby odpowiedzialna za organizację pracy zdalnej ……

Poniższy kwestionariusz identyfikuje ryzyka i zagrożenia związane z wprowadzoną pracą zdalną. Pomaga zweryfikować i zapewnić odpowiednie warunki pracy zdalnej zgodnie uwzględniając:

- zakres zadań i obowiązków na stanowisku pracy
- materiały, narzędzia, urządzenia techniczne niezbędne do wykonywania pracy
- bezpieczeństwo ochrony informacji, bezpieczeństwo danych osobowych
- warunki bhp

Każda odpowiedź pracownika wskaże kierownictwu wyjaśnienie, jakie Pani/Pana zdaniem zagrożenia i ryzyka wystąpią na pracy zdalnej. Pozwoli to ocenić ryzyko, a jeśli zajdzie taka potrzeba – pozwoli przełożonemu podjąć środki minimalizujące ryzyko. Analiza powinna być przeprowadzona indywidualnie dla każdego pracownika składającego wniosek o pracę zdalną, biorąc pod uwagę zadania wynikające z zakresu obowiązków pracownika.

Jeżeli wszystkie odpowiedzi kolumny 4 wynosić będą 0, kartę oceny ryzyka danego pracownika przyjmuje się nie wypełniając kolumn 5,6,7

Jeżeli odpowiedzi kolumny 4 będą różne od 0, należy dokonać indywidualnej oceny ryzyka dla pracownika pracującego zdalnie, określając środki minimalizujące ryzyko i dostosowanie. *Jeśli ryzyko nadal będzie nieakceptowalne – nie ma możliwości wykonywania pracy zdalnej.*

CZĘŚĆ I MOŻLIWOŚCI ORGANIZACYJNE

	WYPEŁNIA PRACOWNIK		WYPEŁNIA KIEROWNIK W POROZUMIENIU Z PRACOWNIKIEM	WYPEŁNIA KIEROWNIK PO USTALENIACH Z PRACOWNIKIEM	WYPEŁNIA KIEROWNIK	
Obszar potencjalnego ryzyka	Czy działanie Panią/a dotyczy? Proszę wpisać **1** = tak, **0** = nie	Czy Pani/a zdaniem to działanie stwarza ryzyko? Proszę wpisać **1** = tak, **0** = nie	Stopień ryzyka 0 – ryzyko dopuszczalne 1 – ryzyko niedopuszczalne	ŚRODKI MINIMALIZUJĄCE RYZYKO (jeżeli trzeba podjąć)	Stopień ryzyka po wdrożeniu środków minimalizujących ryzyko 0 – ryzyko dopuszczalne 1 – ryzyko niedopuszczalne	UWAGI
1	2	3	4	5	6	7
Czy zakres zadań wymaga zabierania dokumentacji lub kopii dokumentacji do domu?						
Czy w czasie wykonywania zadań będzie możliwość bieżącego otrzymywania zdigitalizowanych kopii dokumentów na służbowy e-mail?						
Czy praca wymagała będzie niszczenia dokumentów w domu?						
Czy zakres zadań wymagał będzie przesyłania danych osobowych np. w wiadomościach e-mail?						

Czy zakres zadań obejmuje przetwarzanie danych szczególnie wrażliwych?						
Czy praca wymaga korzystania z prywatnej poczty e-mail oprócz służbowej?						
Czy zakres zadań daje możliwość wykonywania pracy zdalnej w godzinach zgodnych z godzinami pracy Urzędu?						
Inne ryzyko:						

CZĘŚĆ II MOŻLIWOŚCI TECHNICZNE i BEZPIECZEŃSTWO INFORMACJI

	WYPEŁNIA PRACOWNIK		WYPEŁNIA KIEROWNIK W POROZUMIENIU Z PRACOWNIKIEM	WYPEŁNIA KIEROWNIK PO USTALENIACH Z PRACOWNIKIEM	WYPEŁNIA KIEROWNIK	
Obszar potencjalnego ryzyka	Czy działanie Panią/a dotyczy? Proszę wpisać **1** = tak, **0** = nie	Czy Pani/a zdaniem to działanie stwarza ryzyko? Proszę wpisać **1** = tak, **0** = nie	Stopień ryzyka 0 – ryzyko dopuszczalne 1 – ryzyko niedopuszczalne	ŚRODKI MINIMALIZUJĄCE RYZYKO (jeżeli trzeba podjąć)	Stopień ryzyka po wdrożeniu środków minimalizujących ryzyko 0 – ryzyko dopuszczalne 1 – ryzyko niedopuszczalne	UWAGI
1	2	3	4	5	6	7
Czy zakres zadań wymaga wykorzystywania wyłącznie komputera służbowego do zadań służbowych przy pracy zdalnej						
Czy zakres zadań wymaga wykorzystywania wyłącznie telefonu służbowego do zadań służbowych przy pracy zdalnej.						
Czy zakres zadań wymaga wykorzystywania wyłącznie Internetu służbowego do zadań służbowych przy pracy zdalnej.						
Czy łącza internetowe umożliwiają pracę z zapewnieniem płynności transmisji i bezpieczeństwem danych.						
Czy jest możliwe wykonywanie pracy w pomieszczeniu, w którym nie pracują lub przebywają inne osoby w tym domownicy (np. możliwość zapewnienia poufności rozmów telefonicznych).						
Brak możliwości wykonywania dotychczasowych obowiązków w oparciu o dane z zabezpieczonych systemów informatycznych lub zdigitalizowane uprzednio dokumenty.						
Brak możliwości schowania i zabezpieczenia sprzętu po godzinach pracy.						

Zapoznanie pracownika z programami niezbędnymi do wykonywania pracy zdalnej?						
Zapewnione wsparcie informatyczne (zdalne) w przypadku problemów technicznych?						
Inne ryzyko:						

CZĘŚĆ III	**WARUNKI BHP**					
	WYPEŁNIA PRACOWNIK		WYPEŁNIA KIEROWNIK W POROZUMIENIU Z PRACOWNIKIEM	WYPEŁNIA KIEROWNIK PO USTALENIACH Z PRACOWNIKIEM	WYPEŁNIA KIEROWNIK	
Obszar potencjalnego ryzyka	Czy działanie Panią/a dotyczy? Proszę wpisać **1** = tak, **0** = nie	Czy Pani/a zdaniem to działanie stwarza ryzyko? Proszę wpisać **1** = tak, **0** = nie	Stopień ryzyka 0 – ryzyko dopuszczalne 1 – ryzyko niedopuszczalne	ŚRODKI MINIMALIZUJĄCE RYZYKO (jeżeli trzeba podjąć)	Stopień ryzyka po wdrożeniu środków minimalizujących ryzyko 0 – ryzyko dopuszczalne 1 – ryzyko niedopuszczalne	UWAGI
1	2	3	4	5	6	7
Przeprowadzono instruktaż ogólny przed rozpoczęciem pracy.						
Przeprowadzono instruktaż stanowiskowy w dniu przyjęcia pracownika lub po zmianie stanowiska.						
Przeprowadzony instruktaż pracy zdalnej.						
Aktualne szkolenie okresowe BHP.						
Aktualne badania lekarskie (wstępne, okresowe, kontrolne).						
Zapewnione oświetlenie naturalne i sztuczne.						
Czy krzesło spełnia minimalne wymogi bhp na stanowisku pracy przy monitorach ekranowych? - regulacja wysokości siedziska - regulacja oparcia - podłokietniki - podstawa co najmniej pięciopodporowa z kółkami jezdnymi - możliwość obrotu wokół osi pionowej o 360°						
Czy klawiatura stanowi odrębny element wyposażenia podstawowego stanowiska pracy (laptopa)?						

Czy górna krawędź ekranu monitora (laptopa) znajduje się na poziomie lub poniżej oczu pracownika?						
Czy przewody elektryczne są ułożone bezpiecznie? (nie stwarzają zagrożenia potknięciem, nie są narażone na uszkodzenia mechaniczne)						
Inne ryzyko:						

CZĘŚĆ IV	**BEZPIECZEŃSTWO DANYCH (RODO)**					
	WYPEŁNIA PRACOWNIK		WYPEŁNIA KIEROWNIK W POROZUMIENIU Z PRACOWNIKIEM	WYPEŁNIA KIEROWNIK PO USTALENIACH Z PRACOWNIKIEM	WYPEŁNIA KIEROWNIK	
Obszar potencjalnego ryzyka	Czy działanie Panią/a dotyczy? Proszę wpisać **1** = tak, **0** = nie	Czy Pani/a zdaniem to działanie stwarza ryzyko? Proszę wpisać **1** = tak, **0** = nie	Stopień ryzyka 0 – ryzyko dopuszczalne 1 – ryzyko niedopuszczalne	ŚRODKI MINIMALIZUJĄCE RYZYKO (jeżeli trzeba podjąć)	Stopień ryzyka po wdrożeniu środków minimalizujących ryzyko 0 – ryzyko dopuszczalne 1 – ryzyko niedopuszczalne	UWAGI
1	2	3	4	5	6	7
Obszary potencjalnego ryzyka związane z legalnością przetwarzania danych osobowych						
Czy pracownik będzie przetwarzać dane osobowe w ramach pracy zdalnej?						
Czy pracownik będzie przetwarzać dane osobowe szczególnych kategorii lub numery PESEL?						
Czy pracownik został przeszkolony w zakresie ochrony danych osobowych?						
Czy pracownik zobowiązany został do zachowania poufności danych?						
Czy pracownik posiada upoważnienie do przetwarzania danych osobowych we wskazanym zakresie?						
Czy pracownik zapewni ochronę danych osobowych podczas pracy zdalnej, zgodnie z zasadami określonymi w dokumentacji systemu zarządzania bezpieczeństwem informacji obowiązującej w Urzędzie Marszałkowskim Województwa Kujawsko-Pomorskiego w Toruniu?						
Obszary potencjalnego ryzyka związane z bezpieczeństwem danych osobowych						
Utrata, uszkodzenie lub zniszczenie danych osobowych						

(w drodze do/z zdalnego miejsca pracy i na zdalnym stanowisku pracy).						
Nieuzasadniona zmiana danych osobowych.						
Ujawnienie osobom nieuprawnionym lub stworzenie im warunków do pozyskania wiedzy (np. z obserwacji lub dokumentacji) na temat:						
– sposobu działania aplikacji lub systemu informatycznego,						
– stosowanych zabezpieczeń lub/i informacji o sprzęcie i infrastrukturze informatycznej,						
– opuszczenie stanowiska pracy z pozostawieniem dokumentacji biurowej zawierającej dane osobowe z możliwością dostępu do tych informacji przez osoby nieuprawnione,						
– opuszczenie stanowiska pracy z pozostawieniem aktywnej aplikacji umożliwiającej dostęp do zbioru danych osobowych,						
– stworzenie warunków umożliwiających obserwację danych osobowych wyświetlanych na ekranie stanowiska komputerowego przez osoby nieuprawnione (celowe lub nie).						
Obszary potencjalnego ryzyka w zakresie przetwarzania i ochrony danych osobowych						
Dopuszczenie do korzystania z aplikacji umożliwiającej dostęp do danych osobowych przez inne osoby niż osoba, której został przydzielony identyfikator.						
Pozostawienie w miejscu niezabezpieczonym zapisanego identyfikatora lub hasła dostępu do nośników danych osobowych.						
Dopuszczenie do użytkowania sprzętu komputerowego i oprogramowania umożliwiającego dostęp do zbioru danych osobowych przez osoby nieuprawnione.						
Samodzielne instalowanie oprogramowania.						
Samodzielne modyfikowanie parametrów systemu i aplikacji.						
Odczytywanie danych z nośników danych bez uprzedniego przeskanowania programem antywirusowym.						
Sporządzenie kopii danych na nośnikach danych w sytuacjach nieprzewidzianych procedurami przetwarzania i ochrony danych osobowych.						

Utrata kontroli nad nośnikiem danych zawierającym kopię danych osobowych.						
Wady stosowanych technicznych i informatycznych środków bezpieczeństwa.						
Zignorowanie stwierdzenia śladów manipulacji przy komputerze lub programach komputerowych.						
Zignorowanie stwierdzenia obecności urządzeń i programów o nieznanym pochodzeniu.						
Zignorowanie niezapowiedzia-nych zmian w wyglądzie lub zachowaniu wykorzystywanych aplikacji komputerowych lub sprzętu.						
Zignorowanie stwierdzenia nieoczekiwanej, niedającej się wyjaśnić zmiany zawartości bazy danych.						
Zignorowanie obecności na komputerze lub w systemie nieoczekiwanych nowych programów lub zmian konfiguracji oprogramowania.						
Zignorowanie śladów włamania do pomieszczeń, w których prowadzona jest praca zdalna.						
Zignorowanie próby uzyskania hasła dostępu do aplikacji (np. w ramach obsługi technicznej).						
Zignorowanie stwierdzenia nieuzasadnionego przeglądania lub modyfikowania danych w ramach pomocy technicznej.						
Zignorowanie stwierdzenia przeglądania lub modyfikowania danych z użyciem identyfikatora i hasła danego użytkownika przez inną osobę.						
Obszary potencjalnego ryzyka związane z poufnością danych osobowych						
Nieuprawniony dostęp do stanowiska, włamanie do systemu operacyjnego, modyfikacja logów, aplikacji i systemu operacyjnego w celu ujawnienia dokumentów.						
Awarie systemów zabezpieczających stanowisko pracy zdalnej,						
Nieudane testy bezpieczeństwa.						
Błędy i pomyłki administratorów i użytkowników systemu komputerowego.						
Zaniedbania użytkowników						
Wykorzystanie oprogramowania, nośników w sposób nieuprawniony.						
Zagubienie nośnika, dokumentu.						
Włamanie do pomieszczenia, w którym znajduje się system, kradzież urządzeń, nośników, dokumentów,						

Niekontrolowana obecność osób nieuprawnionych w obszarze przetwarzania danych osobowych.						
Niekontrolowane wynoszenie poza obszar przetwarzania danych osobowych nośników informacji i urządzeń mobilnych zawierających dane osobowe.						
Niedyskrecja osób uprawnionych do przetwarzania danych osobowych.						
Skutki wystąpienia incydentu bezpieczeństwa IT.						
Wyłudzenie, fałszowanie dokumentów – nośników haseł						
Nieuprawnione kopiowanie informacji na nośniki danych.						
Naprawy i konserwacje komputerów służących do przetwarzania danych osobowych przez osoby nieuprawnione do przetwarzania danych osobowych.						
Podsłuch lub podgląd danych osobowych.						
Elektromagnetyczna emisja ujawniająca lub podgląd danych przez sieć komputerową/WIFI.						
Obszary potencjalnego ryzyka związane z integralnością danych osobowych						
Uszkodzenie, celowe lub przypadkowe systemu operacyjnego lub urządzeń sieciowych.						
Celowe lub przypadkowe uszkodzenie, zniszczenie lub nieuprawniona modyfikacja danych.						
Przepięcia, wyładowania elektrostatyczne.						
Infekcje wirusowe.						
Awaria sprzętu.						
Pożar, zalanie, ekstremalna temperatura, itp.						
Obszary potencjalnego ryzyka związane z rozliczalnością danych osobowych w systemie informatycznym						
Usunięcie plików lub wykonanie czynności mogącej przerwać lub utrudnić funkcjonowanie systemu.						
Błąd mechanizmu identyfikacji i uwierzytelnienia.						
Nieprzydzielenie użytkownikom indywidualnych identyfikatorów.						
Niewłaściwa administracja systemem informatycznym.						
Niewłaściwa konfiguracja systemu informatycznego.						
Zniszczenie lub zafałszowanie logów systemowych.						
Brak rejestracji udostępniania danych osobowych.						
Podszywanie się pod innego użytkownika.						

Zniszczenie urządzeń, nośników lub dokumentów.						

Na podstawie wyżej udzielonych odpowiedzi i ustalonego ryzyka zawodowego oświadczam, że:

- posiadam/nie posiadam* umiejętności do wykonywania pracy zdalnej w miejscu zamieszkania zgodne z ustalonym zakresem obowiązków;
- posiadam/nie posiadam* możliwości techniczne do wykonywania pracy zdalnej w miejscu zamieszkania spełniające warunki bezpieczeństwa i higieny pracy na stanowisku pracy;
- posiadam/ nie posiadam* możliwości lokalowe do wykonywania pracy zdalnej w miejscu zamieszkania;
- zapoznałem się regulaminem pracy zdalnej Urzędu Marszałkowskiego Województwa Kujawsko-Pomorskiego;
- wyrażam zgodę na przeprowadzanie kontroli w miejscu wykonywania pracy zdalnej przez pracowników wyznaczonych przez pracodawcę.

……..
data i czytelny podpis pracownika

Oświadczam, że dokonałem analizy ryzyka pracy zdalnej pracownika, w tym oceniłem możliwość wykonywania zdalnie zadań wynikających z zakresu obowiązków pracownika. Aktualna ocena ryzyka wykonywanych zadań nie będzie miała wpływu na dotychczasową organizację pracy Urzędu.
Oświadczam, że pracownik został przeszkolony w zakresie wykonywania pracy zdalnej, posiada możliwości i umiejętności do jej samodzielnego wykonywania.

……
data i czytelny podpis bezpośredniego przełożonego

Akceptacja Dyrektora Departamentu

Wyrażam zgodę na wykonywanie pracy zdalnej/Nie wyrażam zgody na wykonywanie pracy zdalnej.*

……..
data i czytelny podpis dyrektora departamentu lub jego zastępcy

Opinia Naczelnika Wydziału Informatyzacji:

*Opiniuję pozytywnie/ Opiniuję negatywnie**

……..
data i czytelny podpis Naczelnika Wydziału Informatyzacji lub upoważnionej osoby

Opinia służby BHP:

*Opiniuję pozytywnie/Opiniuję negatywnie**

……..
data i czytelny podpis pracownika służby BHP

Opinia Inspektora Ochrony Danych:

*Opiniuję pozytywnie/Opiniuję negatywnie**

……..
data i czytelny podpis Inspektora Ochrony Danych lub upoważnionej osoby

Opinia Wydziału Kadr:

*Opiniuję pozytywnie/Opiniuję negatywnie**

……
data i czytelny podpis Naczelnika Wydziału lub upoważnionej osoby

Decyzja Pracodawcy/Sekretarza Województwa:

*Wyrażam zgodę na wykonywanie pracy zdalnej/Nie wyrażam zgody na wykonywanie pracy zdalnej**.

……
data i podpis Pracodawcy/Sekretarza Województwa