załącznik nr 5 do umowy

załącznik nr 10 do   
Polityki Bezpieczeństwa   
Systemu Teleinformatycznego

**Instrukcja telepracy w systemie teleinformatycznym**

W systemie wdraża się niniejszą instrukcję w celu ochrony informacji pobieranych, przetwarzanych lub przechowywanych w miejscach wykonywania telepracy. Pojęcie telepracy odnosi się do wszystkich form pracy poza biurem, w tym do pracy w nietradycyjnych warunkach, o których mówi się: „środowisko zdalnego przetwarzania”, „elastyczne miejsce pracy”, „telepraca” i „praca wirtualna”.

1. Telepraca w ramach Systemu Teleinformatycznego Urzędu jest zabroniona, z wyjątkiem:
   1. dostępu zdalnego w celach administracyjnych ASI oraz osób przez niego wyznaczonych do systemu,
   2. prac serwisowych związanych z realizacją umów utrzymania oprogramowania przez autorów systemów wykorzystywanych w urzędzie,
   3. dostępu do wybranych zasobów przez upoważnione jednostki na podstawie umów powierzenia przetwarzania danych.
   4. sytuacjach opisanych w załączniku nr 6 do Polityki bezpieczeństwa danych osobowych – „*Instrukcja pracy zdalnej wprowadzonej w celu przeciwdziałania COVID-19 zgodnie z art. 3 Ustawy z dnia 2 marca 2020 r. o szczególnych rozwiązaniach związanych z zapobieganiem, przeciwdziałaniem i zwalczaniem COVID-19, innych chorób zakaźnych oraz wywołanych nimi sytuacji kryzysowych*”
2. Zasady określające warunki i ograniczenia dot. korzystania z telepracy dla pkt. 1.1-.1.3 na wybranych zasobach określa *Regulamin korzystania z dostępu do systemu teleinformatycznego Urzędu Miasta Piekary Śląskie*. (będący załącznikiem nr 1 do niniejszej instrukcji).
3. Przekazania loginu i hasła dostępu do systemu teleinformatycznego Urzędu dokonuje się protokołem przekazania podpisywanym przez osobę upoważnioną do dostępu na podstawie zawartych umów.
4. ASI jest odpowiedzialny za poprawną konfigurację środowiska separującą użytkowników zdalnych od innych systemów wewnętrznych nie będących częścią dostępu zdalnego.
5. Użytkownikom zdalnym udostępniane są jedynie zasoby wybrane, wymagane do realizacji zadań.
6. Połączenia i transmisja odbywa się ze wszystkimi ograniczeniami wynikającymi z Polityki stosowanych zabezpieczeń kryptograficznych.
7. W drodze konfiguracji oraz po analizie zakresu w jakim ma być realizowany dostęp zdalny, ASI każdorazowo określa zasady do których musi dopasować się zdalny użytkownik aby mógł pracować na wybranym zasobie systemu.
8. Każdorazowo o dostęp zdalny wnioskuje Naczelnik/Kierownik Urzędu uzyskawszy wcześniej zgodę Prezydenta Miasta (np. poprzez podpisanie umowy powierzenia przetwarzania).
9. Połączenia z systemem mogą być inicjowane tylko i wyłącznie z zabezpieczonych systemów, sieci i stacji oraz tylko w oparciu o szyfrowane tunele wirtualnych sieci prywatnych VPN. Parametry oraz wymagania techniczne co do stosowanych technologii zabezpieczeń dobiera się w oparciu o obowiązujące przepisy prawa, normy polskie oraz zbiór dobrych praktyk a także wytyczne bezpieczeństwa oraz posiadaną wiedzę specjalistyczną ASI lub osoby przez niego wyznaczonej do realizacji tego zadania.
10. Dokłada się wszelkich starań aby całość konfiguracji była spójna i aktualna. W tym celu monitoruje się przyznane dostępy.
11. W razie wątpliwości związanych z bezpieczeństwem przetwarzania ASI może zablokować dostęp celem wyjaśnienia nieprawidłowości.
12. W miarę możliwości technicznych i finansowych dąży się do wprowadzenia rozwiązań technologicznych pozwalających na pełny monitoring wszystkich sesji zdalnych na poziomie każdej wykonywanej operacji, celem jej dokumentowania oraz rozpoczęcia procedury wyjaśniającej w sytuacjach wystąpienia incydentu, w tym także rozpoczęcia procedury wyjaśniającej.
13. Poza tymi szczególnymi zasadami przyjmuje się, że użytkownik pracujący na zasadach telepracy jest użytkownikiem w rozumieniu całej polityki bezpieczeństwa i podlega wszystkim opisanym w niej zasadom, w tym także podlega audytowi zabezpieczeń i kontroli bezpieczeństwa prowadzonymi przez odpowiednie, wyznaczone do tego osoby ze strony Urzędu (ASI, IODO).

Załącznik nr 1 do instrukcji

telepracy w systemie teleinformatycznym

**REGULAMIN KORZYSTANIA Z SYSTEMU TELEINFORMATYCZNEGO URZĘDU MIASTA PIEKARY ŚLĄSKIE**

1. Otrzymując login i hasło dostępu do systemu teleinformatycznego URZĘDU MIASTA PIEKARY ŚLĄSKIE, osoba otrzymująca nabywa możliwość łączenia ze wskazanych zewnętrznych adresów IP poprzez szyfrowany tunel VPN do systemu TI Urzędu.
2. Udzielony dostęp jest oparty o zasadę uprawnień minimalnych. Uprawniona osoba dostaje w ramach uprawnień systemu TI dostęp jedynie do serwerów będących elementem realizacji umowy nr………. z dnia ……..
3. Osoba otrzymująca login i hasło zobowiązana jest do nie ujawniania osobom trzecim danych służących do jego identyfikacji, w szczególności loginu i kodu dostępu oraz innych danych stanowiących tajemnicę.
4. Login i kod dostępu do systemu teleinformatycznego Urzędu mogą być używane tylko i wyłącznie przez osobę, dla której zostały one nadane.
5. Osoba otrzymująca dostęp do systemu TI Urzędu ponosi pełną odpowiedzialność za wszystkie operacje wykonane przy użyciu swojego loginu i hasła.
6. Urząd Miasta Piekary Śląskie nie ponosi odpowiedzialności za skutki wynikłe z ujawnienia osobom trzecim danych służących do identyfikacji w systemie teleinformatycznym Urzędu Miasta Piekary Śląskie.
7. W razie jakichkolwiek podejrzeń, że dostęp do systemy został skompromitowany, administrator sytemu TI Urzędu, może natychmiast zablokować dostęp do takiego konta.
8. W przypadku utraty loginu lub hasła, lub uzasadnionego podejrzenia ujawnienia ich osobom trzecim, właściciel konta jest obowiązany niezwłocznie poinformować o tym fakcie służby informatyczne Urzędu, w celu zablokowania dostępu do systemu teleinformatycznego Urzędu Miasta.
9. Odblokowanie dostępu do systemu teleinformatycznego Urzędu, następuje po pisemnym złożeniu wniosku o ponowne nadanie loginu i hasła do systemu teleinformatycznego Urzędu z powołaniem na odpowiednie umowy.
10. Administrator systemu teleinformatycznego Urzędu ma prawo zablokowania dostępu do konta w systemie teleinformatycznym UM w przypadku stwierdzenia, że osoba posiadająca dostęp korzysta z konta w sposób wskazujący na próby łamania zabezpieczeń lub próby dostępu do danych innych niż wskazane w umowie powierzenia danych.
11. Urząd Miasta Piekary Śląskie nie ponosi odpowiedzialności za brak możliwości korzystania przez osobę posiadającą dostęp do systemu teleinformatycznego Urzędu wynikającej z przyczyn niezależnych od Urzędu lub z innych przyczyn technicznych związanych z funkcjonowaniem systemu teleinformatycznego Urzędu Miasta.
12. Stanowisko na którym będzie uruchomiony dostęp musi bezwzględnie (pod rygorem odłączenia) posiadać aktualną bazę systemu antywirusowego oraz stale aktualizowany system operacyjny z rodziny MS Windows 10/11. Zabrania się korzystania z niespieranych systemów operacyjnych.
13. Służby informatyczne Urzędu mają prawo do przeprowadzenia kontroli spełniania warunków opisanych w punkcie 12. W razie stwierdzenia nieprawidłowości, dostęp może zostać zablokowany do czasu usunięcia wskazanych uchybień.
14. Nie pozostajemy zalogowani w sesjach pulpitów zdalnych serwerów jeśli zakończyliśmy pracę na zasobie - pod groźbą zablokowania dostępu. Konta które będą blokować w ten sposób innym możliwość zalogowania zostaną zablokowane.
15. Zabrania się instalacji i uruchamiania na w/w serwerach jakiegokolwiek dodatkowego oprogramowania firm „trzecich”, bez wcześniejszej zgody Kierownika komórki wł. ds. Informatyki.
16. Wszystkie zapytania oraz nieprawidłowości występujące przy korzystaniu z konta należy zgłaszać za pomocą poczty elektronicznej na adres zi@piekary.pl.