

## INFRASTRUKTURA

1. Administrowanie serwerami i infrastrukturą sieciową Zamawiającego:

- a) Monitorowanie stanu serwerów i usuwanie wszelkich nieprawidłowości w ich pracy;
- b) Konfiguracja sieci, dostępu do Internetu, poczty e-mail itp.;
- c) Instalacja niezbędnego oprogramowania;
- d) Zarządzanie kontami użytkowników na administrowanych serwerach;
- e) Wykonywanie automatycznych kopii bezpieczeństwa danych przechowywanych na serwerach;
- f) Przywracanie prawidłowej pracy serwerów po awariach.

2. Konserwacja i serwis sieci komputerowych wykorzystywanych przez Zamawiającego, za wyjątkiem przypadków, w których prace wykonuje administrator sieci:

- a) Nadzorowanie poprawności działania sieci komputerowej i w razie awarii podjęcie kroków zmierzających do jej usunięcia. W razie konieczności dokonanie zgłoszenia problemu administratorowi sieci;
- b) Podłączanie/odłączanie od sieci komputerowej urządzeń;
- c) Konfiguracja urządzeń sieciowych do potrzeb Zamawiającego.

## OBSŁUGA STACJI ROBOCZYCH, URZĄDZEŃ SIECIOWYCH

1. Obsługa stacji roboczych i urządzeń sieciowych, które nie wymagają zgody i ingerencji autora oprogramowania:

- a) Doradztwo w doborze oprogramowania, nabywanego przez Zamawiającego;
- b) Instalacja oprogramowania i systemów informatycznych na wskazanych stacjach roboczych oraz dokonywanie ich bieżącej aktualizacji;
- c) Instalacja, konfiguracja i zarządzanie oprogramowaniem antywirusowym;
- d) Aktualizacja sterowników;
- e) Serwisowanie oprogramowania i systemów informatycznych – usuwanie usterek, nadzorowanie poprawności wykonywanych kopii bezpieczeństwa baz danych programów, w tym konfiguracja automatycznego tworzenia kopii bezpieczeństwa;
- f) Dobór platformy sprzętowej, komponentów i urządzeń peryferyjnych, a także ich instalacja i konfiguracja;
- h) Informowanie o stwierdzonych nieprawidłowościach w funkcjonowaniu wykorzystywanych programów i systemów;
- i) Nadzorowanie funkcjonowania poszczególnych systemów, w których przetwarzane są dane osobowe, w szczególności w zakresie zarządzania prawami dostępu do tych systemów oraz przeciwdziałaniu nieuprawnionemu dostępowi do systemów, a także podejmowanie

odpowiednich działań w przypadku wykrycia naruszeń w systemie zabezpieczeń;

j) Nadzorowanie instalacji wszelkich modyfikacji oprogramowania wykonywanych przez autora oprogramowania;

k) Nawiązywanie kontaktu z autorem oprogramowania w przypadku wystąpienia awarii, w celu jak najszybszego jej usunięcia.

2. Serwisowanie sprzętu komputerowego:

a) Nadzór nad sprzętem komputerowym i jego okresowa konfiguracja;

b) Dokonywanie wstępnej oceny uszkodzeń sprzętu;

c) Prowadzenie napraw sprzętu komputerowego (z wyłączeniem sprzętu drukującego), które nie wymagają interwencji autoryzowanego serwisu, za wyjątkiem sprzętu objętego gwarancją producenta, który nie podlega żadnym naprawom, z wyłączeniem przypadków zgody producenta i pisemnej akceptacji Zamawiającego; wszystkie podzespoły konieczne do naprawy realizowanej przez zapewnia Zamawiający;

d) Przekazywanie Zamawiającemu podzespołów sprzętu komputerowego, które pozostaną po wykonanej naprawie, wraz z informacją z jakiego sprzętu pochodzą;

e) Wykonywanie czynności serwisowych z należyłą starannością gwarantującą zabezpieczenie przechowywanych tam danych.

#### INNE ZADANIA

1. Ewidencjonowanie oraz zarządzanie licencjami i oprogramowaniem znajdującym się u Zamawiającego, w tym sporządzanie corocznej inwentaryzacji sprzętu;

2. Planowanie polityki IT;

3. Obsługa elektronicznego obiegu dokumentacji, w zakresie współpracy z działem informatyki Urzędu Wojewódzkiego, a także pomoc w obsłudze systemu przez użytkowników;

4. Współpraca z działem informatyki Wielkopolskiego Urzędu Wojewódzkiego;

5. Współpraca z Inspektorem Ochrony Danych Zamawiającego w zakresie ochrony danych, a w szczególności ochrony danych osobowych oraz z Koordynatorem ds. dostępności, w zakresie dostępności cyfrowej;

6. Pomoc przy prowadzonych przez Zamawiającego postępowaniach przetargowych, a w szczególności opracowywanie specyfikacji technicznych na kupowany sprzęt komputerowy i oprogramowanie, weryfikacja otrzymanych ofert pod kątem zgodności z warunkami postępowania;

7. Tworzenie dokumentacji zgodnie z procedurami obowiązującymi u Zamawiającego;

8. Kontrola

a) wprowadzenie zwiększonej kontroli stanu bezpieczeństwa systemów teleinformatycznych;

b) monitorowanie i weryfikowanie, czy nie doszło do naruszenia bezpieczeństwa komunikacji elektronicznej;

c) sprawdzanie dostępności usług elektronicznych;

d) dokonywanie, w razie potrzeby, zmian w dostępie do systemów;

e) informowanie personelu Zamawiającego (w szczególności odpowiedzialnych za

- bezpieczeństwo systemów) o konieczności zachowania zwiększonej czujności w stosunku do stanów/sytuacji odbiegających od normy;
- g) weryfikowanie posiadanych kopii zapasowych systemów w stosunku do systemów teleinformatycznych wchodzących w skład infrastruktury krytycznej oraz systemów kluczowych dla funkcjonowania Przedsiębiorstwa;
- h) weryfikowanie czasu wymaganego na przywrócenie poprawności funkcjonowania systemu;
- i) sprawdzanie aktualnego stanu bezpieczeństwa systemów i ocena wpływu zagrożenia na bezpieczeństwo teleinformatyczne na podstawie bieżących informacji i prognoz wydarzeń;
- j) informowanie na bieżąco o efektach przeprowadzonych działań kierownika Zamawiającego;
- k) zapewnienie dostępność w trybie alarmowym personelu odpowiedzialnego za bezpieczeństwo systemów;
- l) dokonywanie przeglądu dostępnych zasobów zapasowych pod względem możliwości wykorzystania w przypadku zaistnienia ataku;
- m) przygotowanie do uruchomienia planów umożliwiających zachowanie ciągłości działania po wystąpieniu potencjalnego ataku, w tym min.: dokonywanie przeglądu i ewentualnego audytu planów awaryjnych oraz infrastruktury teleinformatycznej, w tym wyznaczenie systemów kluczowych do utrzymania ciągłości pracy;
- n) przygotowanie ograniczenia operacji na serwerach, w celu możliwości ich szybkiego i bezawaryjnego zamknięcia i pozostawienie dostępu wyłącznie użytkownikom wytypowanym przez administratora.

Dodatkowe warunki realizacji umowy:

1. Pełnienie dyżuru w ilości 40 godzin miesięcznie, wg ustalonego grafiku przez Zamawiającego i Wykonawcę.
2. Realizowanie w ramach umowy telefonicznej obsługi tzw. HelpDesk, w pracy Przedsiębiorstwa tj. od poniedziałku do piątku w godzinach 7:00 – 16:00.
3. Zapewnienie tzw. pogotowia serwisowego, w ramach którego określa się gwarantowany maksymalny czas reakcji na usunięcie awarii systemu komputerowego lub innej awarii o charakterze krytycznym do 4h w trakcie dnia roboczego oraz określa się gwarantowany do 48h maksymalny czas reakcji na usunięcie innych awarii lub usterek, których powstanie nie spowoduje istotnych negatywnych następstw w funkcjonowaniu systemów i urządzeń, a ich naprawa nie musi następować niezwłocznie – licząc od momentu przyjęcia telefonicznego bądź pisemnego zgłoszenia awarii. Poprzez czas reakcji Zamawiający rozumie czasokres, w przeciągu którego nastąpi reakcji w postaci fizycznego stawienia się do siedziby Zamawiającego, celem zdiagnozowania powstałego problemu i usunięcia awarii, bądź przystąpienia do rozpoczęcia prac

związanych z usuwaniem awarii.

Zamawiający dopuszcza również konsultacje zdalne w przypadku, gdy awarię uda się zdiagnozować zdalnie. Jeżeli natomiast po konsultacji zdalnej nie uda się zdiagnozować przyczyny awarii o charakterze krytycznym, zapewnienie gwarancji w przeciągu 4h, fizycznego pojawienia się w siedzibie Zamawiającego celem zdiagnozowania i usunięcia awarii.