Załącznik nr 7 do SWZ

**Opis przedmiotu zamówienia**

**(zakres usług informatycznych, warunki ich świadczenia oraz wymagania stawiane Wykonawcy)**

1. **Ogólny opis systemu informatycznego**

Systemu informatyczny eksploatowany jest w jednej lokalizacji – Warta Bolesławiecka 40C i składa się z następujących elementów:

* liczba stacji roboczych: 33 szt.;
* liczba laptopów: 18 szt.,
* liczba drukarek: 33 szt.;
* liczba serwerów fizycznych: 3 szt.;
* liczba serwerów wirtualnych: 6 szt.;
* liczba pamięci sieciowych: 2 szt.;
* liczba punktów dostępu bezprzewodowego: 2 szt.;
* liczba przełączników (w tym zarządzalne): 4 szt.;
* liczba urządzeń brzegowych (UTM): 1 szt.;
* rodzaj wykorzystywanych baz danych: DBF, MDB, SQL (MySQL, Firebird), Lotus;
* systemy operacyjne serwerów: MS Windows, CENTOS, Debian,

1. **Wykaz użytkowanego oprogramowania dziedzinowego i bazodanowego**

Zamawiający wymaga umiejętności instalacji i konfiguracji oraz znajomości zagadnień merytorycznych następujących programów:

1) Programy SIGID w modułach:

a) ewidencja opłat za wieczyste użytkowanie,

b) ewidencja i rozliczanie opłat za gospodarowanie odpadami,

c) ewidencja środków trwałych i wyposażenia,

d) ewidencja opłat dzierżawnych,

e) ewidencja i rozliczanie podatku vat,

f) ewidencja i drukowanie faktur,

g) programy obsługi kasy,

h) księgowość budżetowa jednostki,

i) gospodarka materiałowa jednostek budżetowych,

j) podatek od nieruchomości dla osób prawnych,

k) ewidencja i rozliczanie innych opłat,

l) kadry i płace urzędu,

m) podatek od środków transportowych,

n) podatek rolny/leśny/nieruch. dla osób fizycznych

o) podatek rolny/leśny dla osób prawnych

2) Gminny Portal Podatkowy „SIGID”

3) elektroniczny obieg dokumentów - URZĘDY2020,

4) System Informacji Przestrzennej GIS „GIAP”,

5) System ŹRODŁO,

6) System monitorowania urządzeń sieciowych (ZABBIX),

7) System agregowania logów z urządzeń sieciowych (GrayLog).

1. **Zasady świadczenia usług informatycznych**

* miejsce wykonywania: Urząd Gminy Warta Bolesławiecka;
* sposób realizacji: dwa razy w tygodniu w dni ustalone z Zamawiającym (4 godziny pracy informatyka podczas każdej wizyty) w tym dwie wizyty miesiącu w obsadzie dwuosobowej;
* koszt dojazdów do Zamawiającego pokrywa Wykonawca;
* przystąpienie do usuwania awarii krytycznych w czasie zadeklarowanym w ofercie, za pośrednictwem połączeń zdalnych oraz w razie potrzeby w siedzibie Zamawiającego (jako awarię krytyczną rozumie się zdarzenie uniemożliwiających lub utrudniające pracę użytkowników w systemie informatycznym);
* przystąpienie do usuwania awarii innych niż krytyczne w czasie nie dłuższym niż 4 godziny od chwili zgłoszenia (za pośrednictwem połączeń zdalnych oraz w razie potrzeby w siedzibie Zamawiającego);
* wykonywanie prac serwisowych oraz usuwanie awarii według potrzeb Zamawiającego;
* wykonywanie prac serwisowych przez więcej niż jednego pracownika (maksymalnie 3 osoby) w przypadkach zwiększonego zapotrzebowania na usługi informatyczne – Zamawiający powiadomi Wykonawcę o takiej konieczności z min. dwudniowym wyprzedzeniem;
* Wykonawca zapewnia licencjonowany program do wykonywania połączeń zdalnych w oparciu o łącza szyfrowane (legalność programu potwierdzona zostanie przez Wykonawcę po zawarciu umowy na obsługę informatyczną).

1. **Obsługa podstawowa**
2. Zakres podstawowy:
3. administrowanie lokalną siecią komputerową polegające min. na utrzymaniu sprawności urządzeń aktywnych (przełączniki, routery/UTM-y, punktu dostępu bezprzewodowego, kontrolery) oraz konfiguracji stosownie do potrzeb Zamawiającego;
4. administrowanie urządzeniami komputerowymi (min. serwery, komputery, laptopy, drukarki) polegające min. na utrzymaniu ich sprawności, regularnej aktualizacji zainstalowanego oprogramowania oraz instalacji i konfiguracji stosownie do potrzeb Zamawiającego;
5. instalacja i konfiguracja nowego sprzętu komputerowego (przenoszenie danych);
6. zabezpieczenie infrastruktury przed nieuprawnionym dostępem w tym zarządzanie mechanizmem autoryzacji użytkowników oraz politykami bezpieczeństwa urządzenia brzegowego;
7. okresowe wykonywanie przeglądów i konserwacji baz danych (zgodnie z zaleceniami dostawców oprogramowania);
8. zabezpieczenie danych gromadzonych na serwerach przed ich utratą, w tym codzienne sporządzanie kopii awaryjnych zgodnie z zasadami określonymi przez Zamawiającego;
9. archiwizowanie baz danych na płytę CD/DVD jeden raz w miesiącu;
10. archiwizowanie baz, których wielkość przekracza pojemność płyty DVD, na nośniku zewnętrznym (dysku usb) nie rzadziej niż jeden raz w miesiącu;
11. wykonywanie min. jeden raz na trzy miesiące kopii maszyn wirtualnych na zaszyfrowanym dysku zewnętrznym;
12. zabezpieczanie danych gromadzonych na stacjach roboczych zgodnie z zasadami określonymi przez Zamawiającego;
13. pomoc pracownikom w rozwiązywaniu problemów w użytkowaniu programów biurowych i użytkowych;
14. wykonywanie czynności informatycznych zgodnie z obowiązującymi przepisami dotyczącymi ochrony danych osobowych i regulacjami wewnętrznymi Zamawiającego dotyczącymi bezpieczeństwa danych i informacji;
15. współpraca z Inspektorem Ochrony Danych;
16. wykonywanie podstawowych prac serwisowych w siedzibie Zamawiającego w tym wymiana uszkodzonych podzespołów – koszt zakupu podzespołów ponosi Zamawiający;
17. konfiguracja i weryfikacja mechanizmu wymuszenia okresowej zmiany haseł do systemów operacyjnych stacji roboczych oraz aplikacji zgodnie z zasadami przyjętymi przez Zamawiającego;
18. wykonywanie zdalnego serwisu i pomocy technicznej za pomocą połączeń szyfrowanych;
19. zagwarantowanie jak najszybszego przywrócenia pełnej sprawności systemu informatycznego w przypadku wystąpienia awarii;
20. obsługa techniczna (instalacja, aktualizacja, konfiguracja i administracja) programów użytkowych;
21. przygotowanie opinii technicznych i zaleceń dotyczących systemu informatycznego;
22. pomoc w doborze nowych rozwiązań informatycznych oraz planowanie rozwoju systemu informatycznego;
23. blokowanie stron internetowych, adresów i programów wskazanych przez Zamawiającego;
24. blokowanie lub ograniczanie dostępu do Internetu z komputerów wskazanych przez Zamawiającego;
25. konfiguracja skrzynek poczty elektronicznej zgodnie z wymogami Zamawiającego;
26. usuwanie danych z nośników przeznaczonych do likwidacji lub przekazania,
27. konsultacje telefoniczne;
28. reprezentowanie Zamawiającego na spotkaniach dot. rozwoju i wdrożenia technik komputerowych;
29. przestrzeganie zasad wprowadzonych przez Zamawiającego w Polityce Ochrony Danych Osobowych;
30. analiza Polityki Ochrony Danych Osobowych wprowadzonej przez Zamawiającego oraz proponowanie modyfikacji w celu poprawy bezpieczeństwa systemu informatycznego;
31. wykonywanie połączeń zdalnych do systemu informatycznego Zamawiającego wyłącznie z zachowaniem zasad określonych przez Zamawiającego w Polityce Ochrony Danych Osobowych z wykorzystaniem legalnego oprogramowania gwarantującego szyfrowanie takiego połączenia.
32. Zakres rozszerzony (kontrola zabezpieczeń systemu informatycznego):
33. regularne (nie rzadziej niż jeden raz w miesiącu) monitorowanie wolnej przestrzeni dyskowej dysków sieciowych oraz serwerów;
34. regularne (nie rzadziej niż jeden raz w miesiącu) monitorowanie wykorzystania mocy obliczeniowej serwerów oraz zajętości pamięci RAM;
35. okresowe (nie rzadziej niż jeden raz na trzy miesiące) sprawdzenie poprawności odtworzenia kopii zapasowych (dotyczy programów i danych dla których wykonanie takiej czynności jest możliwe do wykonania w oparciu o posiadane przez Zamawiającego urządzenia);
36. okresowe (nie rzadziej niż jeden raz w miesiącu) kontrolowanie daty wykonania kopii maszyn wirtualnych na dyskach sieciowych;
37. okresowe sprawdzanie sprawności baterii zainstalowanych w ups-ach;
38. zablokowanie serwerom i pamięciom sieciowym bezpośredniego dostępu do sieci Internet oraz okresowe przywracanie takiego dostępu w celu wykonania aktualizacji oprogramowania,
39. regularna aktualizacja (zgodnie z zasadami uzgodnionymi z Zamawiającym) najważniejszych programów zainstalowanych na stacjach roboczych;
40. regularna aktualizacja (nie rzadziej niż raz na 3 miesiące) oprogramowania firmware urządzeń sieci LAN (router, przełączniki zarządzalne, punkty dostępu bezprzewodowego, kontrolery);
41. zmiana haseł domyślnych wszystkich urządzeń sieciowych oraz przekazanie tych haseł Zamawiającemu;
42. utrzymywanie opisu aktualnej konfiguracji systemu informatycznego oraz wykorzystywanych haseł administracyjnych;
43. przechowywanie kopii zapasowej plików konfiguracyjnych urządzeń sieciowych takich jak router/UTM, przełącznik zarządzalny, punkt dostępu bezprzewodowego, kontroler WiFi; pliki muszą zawierać ostatnią poprawną konfigurację urządzeń;
44. okresowa (nie rzadziej niż jeden raz w roku) weryfikacja uprawnień w systemach informatycznych (zakres i sposób realizacji określi Zamawiający);
45. utrzymanie aktualnego spisu sprzętu komputerowego z wyszczególnieniem jego parametrów technicznych (oprogramowanie do prowadzenia takiej ewidencji zapewni Zamawiający);
46. prowadzenie ewidencji oprogramowania zainstalowanego na stacjach roboczych i serwerach (oprogramowanie do prowadzenia takiej ewidencji zapewni Zamawiający);
47. prowadzenie wykazu oprogramowania dopuszczonego do stosowania w jednostce,
48. okresowe (nie rzadziej niż jeden raz w miesiącu) skanowanie sieci LAN w poszukiwaniu obcych urządzeń i udostępnionych udziałów,
49. okresowe (nie rzadziej niż jeden raz w miesiącu) sprawdzenie urządzeń podłączonych do sieci bezprzewodowej (klientów WiFi),
50. blokada dostępu do nośników pamięci zgodnie ze wskazaniami Zamawiającego (oprogramowanie do wykonania blokad dostarczy Zamawiający),
51. szyfrowanie danych/dysków komputerów przenośnych oraz pamięci usb zgodnie ze wskazaniami Zamawiającego;
52. izolacja ruchu w sieci LAN w przypadku konieczności udzielenia dostępu do Internetu osobom nieuprawnionym do korzystania z zasobów sieci lokalnej;
53. ograniczenie dostępu do zasobów sieci LAN za pośrednictwem gniazd sieci komputerowej i urządzeń sieciowych w pomieszczeniach ogólnodostępnych;
54. dezaktywacja usług i serwisów lokalnego systemu informatycznego, które umożliwiają logowanie się do programu lub urządzenia bez użycia mechanizmów szyfrowania (np. ftp, telnet, http);
55. prowadzenie dziennika systemów informatycznych i umieszczanie w nim wpisów dotyczących najważniejszych wydarzeń i czynności, które mają związek z funkcjonowaniem systemu informatycznego (aktualizacje, awarie i uszkodzenia, połączenia zdalne ASI, zmiany konfiguracji); w przypadku gdy dziennik prowadzony jest w wersji elektronicznej Wykonawca zobowiązany jest przedłożyć Zamawiającemu jeden raz w miesiącu wyciąg takiego rejestru w postaci pliku PDF;
56. analiza wprowadzonych przez Zamawiającego wewnętrznych regulacji dotyczących ochrony danych i informacji oraz proponowanie ich modyfikacji w celu poprawy bezpieczeństwa systemu informatycznego;
57. przeprowadzanie szkoleń z zakresu bezpieczeństwa informacji dla pracowników Zamawiającego (o terminie takiego szkolenia Zamawiający powiadomi wykonawcę z trzydniowym wyprzedzeniem)
58. **Obsługa dodatkowa:**

Usuwanie awarii i wykonywanie innych usług doraźnych w dniach nieobjętych obsługą

podstawową - w przypadkach krytycznych uniemożliwiających pracę.

1. **Pozostałe wymagania dotyczące Wykonawcy:**

* dobra znajomość przepisów i zagadnień związanych z ochroną danych osobowych;
* dobra znajomość języka zapytań SQL;
* Wykonawca musi posiadać certyfikat ukończenia szkolenia z administracji MS Windows Server;
* Wykonawca musi posiadać certyfikat ukończenia szkolenia z zakresu instalacji i konfiguracji przełączników zarządzalnych firmy DCN;
* Wykonawca musi posiadać certyfikat ukończenia szkolenia z zakresu instalacji i konfiguracji serwerów maszyn wirtualnych w środowisku CITRIX XEN Server;
* Wykonawca musi posiadać certyfikat ukończenia szkolenia z administracji i konfiguracji urządzenia UTM STORMSHIELD;
* Wykonawca musi posiadać certyfikaty ukończenia szkoleń z zakresu bezpieczeństwa informacji (w oparciu o normę ISO 27001) oraz potwierdzające znajomość zagadnień cyberbezpieczeństwa;
* Wykonawca musi posiadać certyfikat potwierdzający znajomość instalacji i konfiguracji systemu ZABBIX;
* Certyfikaty ukończenia szkoleń muszą być wystawione przez producenta systemu/urządzenia lub jego przedstawiciela, autoryzowane centrum szkoleniowe lub podmiot, którego głównym zakresem działania jest przeprowadzanie szkoleń informatycznych;
* Wykonawca musi posiadać minimum 5 letnie doświadczenie w obsłudze informatycznej urzędów miast i gmin; wymagane referencje (3 sztuki),
* Wykonawca musi dysponować doświadczoną kadrą informatyczną zapewniającą stałą i sprawną obsługę (min. 4 informatyków zatrudnionych na podstawie umowy o pracę).