Gmina Dmosin
Dmosin 09
95-061 Dmosin

ZAPYTANIE OFERTOWE

Zwracamy się z prośbą o przedstawienie swojej oferty na poniżej opisany przedmiot zamówienia:

Dostawa oprogramowania do kompleksowego zarządzania siecią i infrastrukturą IT Urzędu Gminy w Dmosinie zamawianych w ramach realizacji Konkursu Grantowego Cyfrowa Gmina, Oś V. Rozwój cyfrowy JST oraz wzmocnienie cyfrowej odporności na zagrożenia - REACT-EU, Działanie 5.1 Rozwój cyfrowy JST oraz wzmocnienie cyfrowej odporności na zagrożenia, Program Operacyjny Polska Cyfrowa na lata 2014 – 2020".
Termin realizacji zamówienia 30 dni od podpisania umowy
Kryterium oceny ofert – cena 100%

Inne istotne warunki zamówienia przyszłej umowy, a w szczególności warunki zapłaty

Dostawa oprogramowania do kompleksowego zarządzania siecią i infrastrukturą IT Urzędu Gminy w Dmosinie zamawianych w ramach realizacji Konkursu Grantowego Cyfrowa Gmina, Oś V. Rozwój cyfrowy JST oraz wzmocnienie cyfrowej odporności na zagrożenia - REACT-EU, Działanie 5.1 Rozwój cyfrowy JST oraz wzmocnienie cyfrowej odporności na zagrożenia, Program Operacyjny Polska Cyfrowa na lata 2014 – 2020".

Informacje podstawowe:

1) Termin realizacji zamówienia: 7 dni od podpisania umowy,
2) Każdy z oferentów może złożyć tylko jedną ofertę,
3) Kryterium wyboru oferty: najniższa cena brutto,
4) Oferty złożone po terminie nie będą rozpatrywane,
5) W postępowaniu mogą brać udział Wykonawcy, którzy nie podlegają wykluczeniu z postępowania na podstawie art. 7 ust. 1 ustawy z dnia 13 kwietnia 2022r. o szczególnych rozwiązaniach w zakresie przeciwdziałania wspieraniu agresji na Ukrainę oraz służących ochronie bezpieczeństwa narodowego (Dz.U. z 2022r. poz.835).
6) Zamawiający zgodnie z art. 7 ust. 3 ustawy z dnia 13 kwietnia 2022r. o szczególnych rozwiązaniach w zakresie przeciwdziałania wspieraniu agresji na Ukrainę oraz służących ochronie bezpieczeństwa narodowego (Dz.U. z 2022r. poz.835) odrzuci ofertę Wykonawcy, który podlega wykluczeniu na podstawie art.7 ust.1 w/w ustawy. Osoba lub podmiot podlegające wykluczeniu na podstawie art.7 ust.1 w/w ustawy, które w okresie tego

wykluczenia ubiegają się o udzielenie zamówienia publicznego podlegają karze pieniężnej w wysokości do 20 000 000 zł, o czym stanowi art.7 ust.6 i 7 powołanej ustawy.

7) Zamawiający zastrzega sobie prawo odwołania postępowania lub jego zamknięcia bez wybrania którejkolwiek ze złożonych ofert.

I. Przedmiot zamówienia:

Dostawa oprogramowania do kompleksowego zarządzania siecią i infrastrukturą IT Urzędu Gminy w Dmosinie w ramach realizacji Konkursu Grantowego Cyfrowa Gmina, Oś V. Rozwój cyfrowy JST oraz wzmocnienie cyfrowej odporności na zagrożenia - REACT-EU, Działanie 5.1 Rozwój cyfrowy JST oraz wzmocnienie cyfrowej odporności na zagrożenia, Program Operacyjny Polska Cyfrowa na lata 2014 – 2020.

II. Wymagania ogólne do przedmiotu zamówienia:

1. Oprogramowanie w polskiej wersji językowej,
2. Ilość licencji na oprogramowanie: 25 stacji roboczych,
3. Licencja wieczysta,
4. Stan licencji: nowa licencja,
5. Zastosowanie licencji: licencja komercyjna,
6. Darmowe aktualizacje i pomoc techniczna przez okres minimum 12 miesięcy,
7. Oferowane oprogramowanie posiada Podręcznik Użytkownika/instrukcję obsługi w języku polskim,
8. Praca z systemami operacyjnymi z rodziny Windows,
9. Oprogramowanie zgodne z wymogami RODO,
10. Oprogramowanie posiada budowę modułową, możliwość dowolnego wyboru modułów,
11. Budowa oparta o serwer zarządzający, zdalne konsole oraz Agentów,
12. Komunikacja pomiędzy Serwerem, a Agentami i Konsolami nawiązywana przy użyciu szyfrowanego protokołu TLS 1.2,
13. Ochrona Agenta przed usunięciem,
14. Wykorzystanie przez program darmowego silnika bazy danych z kodem źródłowym dostępnym na licencji open-source – nie wymaga dodatkowego licencjonowania,
15. Brak limitu ilości danych dla baza danych,
16. Dane dotyczące działań pracownika na komputerze (np. historia aktywności, polityka korzystania z Internetu oraz aplikacji, dostęp do zewnętrznych nośników danych itp.) są odseparowane od danych stricte technicznych tj. informacji o stacji roboczej i są grupowane w osobnym, dedykowanym oknie,
17. Dostęp do danych osobowych oraz danych z monitoringu, zgodnie z RODO, objęty jest kontrolą na poziomie wybranych Administratorów,

18. Możliwość zarządzania przez głównego Administratora uprawnieniami konfiguracyjnymi programu dla innych kont z rolą administracyjną (m.in. możliwość wyłączenia zdalnej deinstalacji Agenta, ograniczenie dostępu do opcji programu),
19. Logowanie działań administratorów,
20. Program posiada dziennik z listą czynności wykonanych przez administratorów, które zmodyfikowały obiekty znajdujące się w systemie w tym m.in. logowanie dostępu do Opcji programu, logowanie dostępu do informacji o aktywności użytkownika, logowanie poleceń deinstalacji Agenta,
21. Działania administratorów mogą być automatycznie eksportowane do zewnętrznego kolektora Syslog,
22. Możliwość nadawania w programie kontom administracyjnym różnych poziomów dostępu oraz uprawnień zarówno do funkcji Programu, grup urządzeń, jak i użytkowników,
23. Możliwość jednoczesnej pracy wielu Administratorów,
24. Zarządzanie hierarchią użytkowników (w tym import z Active Directory);

III. Wymagania szczegółowe - opis wymaganych modułów:

1. Moduł do monitorowania infrastruktury sieciowej i wizualizacji sieci:
   1) Wykrywanie urządzeń w sieci poprzez skanowanie ping oraz arp-ping,
   2) Wykrywanie urządzeń na podstawie informacji odczytanych z Active Directory (wraz z informacją o OU),
   3) Wizualizacja stanu urządzeń w postaci ikon urządzeń na graficznych mapach sieci,
   4) Wizualizacja map urządzeń poprzez tworzenie spersonalizowanych map z dowolnym kolorem tła,
   5) Wizualizacja map urządzeń poprzez tworzenie spersonalizowanych map z wykorzystaniem jako tła zaimportowanych obrazków (np. schematu rozmieszczenia pomieszczeń w budynku),
   6) Wizualizacja map urządzeń poprzez grupowanie urządzeń na narysowanych polach o dowolnym rozmiarze i kolorze,
   7) Wizualizacja map urządzeń poprzez wstawianie dowolnego tekstu na mapie,
   8) Wizualizacja połączeń pomiędzy urządzeniami a przełącznikami za pomocą linii i informacji, do którego portu przełącznika podłączone jest dane urządzenie w sposób manualny oraz automatyczny,
   9) Zablokowanie mapy urządzeń przed przypadkową edycją,
   10) Monitorowanie serwisów TCP/IP, HTTP, POP3, SMTP, FTP i innych wraz z możliwością definiowania własnych serwisów. Program ma monitorować czas ich odpowiedzi i procent utraconych pakietów,
   11) Monitorowanie serwerów pocztowych w zakresie:
      a) czasu logowania do serwisu odbierającego oraz czasu wysyłania poczty,
      b) stanu systemów i wysyłania powiadomienia (e-mail, SMS i inne), w razie gdyby przestały one odpowiadać lub funkcjonowały wadliwie (np. gdy ważne parametry znajdą się poza zakresem),
      c) możliwość wykonywania operacji testowych,

d) możliwość wysłania powiadomienia jeśli serwer pocztowy nie działa,

12) Monitorowanie serwerów WWW i adresów URL,

13) Cykliczne monitorowanie czasu ładowania strony internetowej, zmiany treści na stronie internetowej i statusu protokołu HTTPS,

14) Monitorowanie w zakresie obsługi szyfrowania SSL/TLS w powiadomieniach e-mail,

15) Monitorowanie w zakresie obsługi urządzeń SNMP wspierających SNMP v1/2/3 z szyfrowaniem oraz autoryzacją, (np. przełączniki, routery, drukarki sieciowe, urządzenia VoIP itp.) – monitorowanie wartości za pomocą nazw zmiennych oraz OID,

16) Monitorowanie obsługi komunikatów syslog i pułapek SNMP i ewidencjonowanie odebranych z nich danych,

17) Monitoring routerów i przełączników wg:

a) zmian stanu interfejsów sieciowych,

b) ruchu sieciowego,

c) podłączonych stacji roboczych – graficzna prezentacja panelu switcha,

d) ruchu generowanego przez podłączone do portów stacje robocze,

18) Monitorowanie serwisów Windows - monitor serwisów Windows alarmuje, gdy serwis przestanie działać oraz pozwala na jego uruchomienie/zatrzymanie/zrestartowanie,

19) Wyświetlanie statystyk przy każdym urządzeniu na mapie takich jak: czas odpowiedzi urządzenia, czas od ostatniej poprawnej odpowiedzi, nazwa DNS, adres IP, status zarządzalności SNMP, ostrzeżenie o zdarzeniu na urządzeniu,

20) Monitorowanie wydajności systemów Windows (obciążenie CPU, pamięci, zajętość dysków, transfer sieciowy);

Inne funkcje modułu:

1) Program ma posługiwać się inteligentnymi mapami i oddziałami służącymi do lepszego zarządzania logiczną strukturą urządzeń w urzędzie oraz tworzyć dynamiczne mapy wg własnych filtrów,

2) Program ma mieć funkcję kompilatora plików MIB, który umożliwia dodawanie definicji dla modułów SNMP,

3) Program ma umożliwiać nakładanie na urządzenia liczników wydajności WMI oraz SNMP wg szablonów definiowania alarmów z wykorzystaniem akcji związanych ze zdarzeniami w systemie, m.in.: wysłanie komunikatu pulpitowego, wysłanie wiadomości e-mail, wysłanie SMS, uruchomienie programu, wysłanie pułapki SNMP, wysłanie pakietu Wake-On-LAN, zatrzymanie/restart usługi Windows, wyłączenie/restart komputera,

4) Możliwość budowania przez Administratora w/w alarmów z wykorzystaniem ciągu przyczynowo skutkowego (Administrator samodzielnie może wskazać dowolne zdarzenie z listy, którego wykrycie wzbudzi alarm oraz dowolną liczbę akcji wybranych z listy, które zostaną wykonane jako reakcja na wykryte zdarzenie.),

5) Możliwość ewentualnej integracji ze sprzętową bramką GSM w celu wysyłania powiadomień SMS z wykorzystaniem protokołu netGSM (SOAP);

2. Moduł do inwentaryzacji sprzętu i oprogramowania:

   1) Automatyczne gromadzenie przez program informacje o sprzęcie i oprogramowaniu na stacjach roboczych,
   2) Prezentowanie przez program szczegółów dotyczących sprzętu: modelu, procesora, pamięci, płyty głównej, napędów, kart itp.,
   3) Inwentaryzacja ma obejmować m.in.: zestawienie posiadanych konfiguracji sprzętowych, wolne miejsce na dyskach, średnie wykorzystanie pamięci, informacje pozwalające na wytypowanie systemów, dla których konieczny jest upgrade,
   4) Informowanie o zainstalowanych aplikacjach oraz aktualizacjach Windows, co bezpośrednio umożliwia audytowanie i weryfikację użytkowania licencji w organizacji,
   5) Zbieranie informacji w zakresie wszystkich zmian przeprowadzonych na wybranej stacji roboczej: instalacji/deinstalacji aplikacji, zmian adresu IP itd.,
   6) Posiadanie możliwości wysyłania powiadomienia np. e-mailem w przypadku zainstalowania programu lub jakiejkolwiek zmiany konfiguracji sprzętowej komputera,
   7) Możliwość odczytanie numeru seryjnego (klucze licencyjne),
   8) Możliwość automatycznego zarządzania instalacjami i deinstalacjami oprogramowania poprzez określenie paczek aplikacji wymaganych oraz nieautoryzowanych,
   9) Możliwość przeglądu informacji o konfiguracji systemu, np. komend startowych, zmiennych środowiskowych, kontach lokalnych użytkowników, harmonogramie zadań itp.,
   10) Możliwość tworzenia listy plików użytkowników z określonym rozszerzeniem (np. filmy .AVI) znalezionych na stacjach roboczych oraz ich zdalne usuwanie wraz z wykrywaniem metadanych plików użytkownika: obrazów (wymiary obrazka), video (długość filmu), audio (długość nagrania), archiwów (liczba plików w środku, rozmiar po wypakowaniu),
   11) Możliwość wymiany plików do i ze stacją roboczą poprzez funkcję Menedżera plików. Działania administratorów wykonywane w tej funkcji są logowane;

Moduł inwentaryzacji zasobów ma umożliwiać prowadzenie bazy ewidencji majątku IT w zakresie sprzętu i programowania:

   1) Przechowywania wszystkich informacji dotyczących infrastruktury IT w jednym miejscu oraz automatycznego aktualizowania zgromadzonych informacji,
   2) Tworzenia powiązań między zasobami a urządzeniami,
   3) Tworzenia powiązań między zasobami a kontami użytkowników (zarówno lokalnymi, jaki zsynchronizowanymi z Active Directory), wskazywanie osób odpowiedzialnych,
   4) Wskazania osób uprawnionych do użycia zasobów,
   5) Definiowania własnych typów zasobów (elementów wyposażenia), ich atrybutów oraz wartości dla danego urządzenia lub oprogramowania, możliwość dodawania dodatkowych informacji, np. numer inwentarzowy, osoba odpowiedzialna, numer dokumentu zakupu, wartość sprzętu lub oprogramowania, nazwa sprzedawcy, termin upływu gwarancji, termin kolejnego przeglądu (można podać datę, po której administrator otrzyma powiadomienie e-mail zbliżającym się terminie przeglądu lub upływie gwarancji), nazwa firmy serwisującej lub własny komentarz,
   6) Określenia atrybutów wymaganych, które są obowiązkowe dla wszystkich zasobów,
   7) Określenia atrybutów dodatkowych tylko dla wybranych typów zasobów,

8) Definiowania własnych list jednokrotnego wyboru jako dodatkowych informacji o zasobie,
9) Importu danych z zewnętrznego źródła (.CSV),
10) Przechowywania dowolnych dokumentów (np. pliki .DOCX, .XLSX, .PDF), np.: skan faktury zakupu, gwarancji, dowolnego dokumentu itp.,
11) Tworzenia powiązań między zasobami a dokumentami w relacji 1:N,
12) Oznaczania statusów zasobów, np. w użyciu, w naprawie, zutylizowany itp.,
13) Ewidencji czynności wykonywanych na zasobach, np.: aktualizacja, naprawa w serwisie, konserwacja itp. wraz z możliwością określenia kosztu oraz czasu przeznaczonego na wykonanie czynności,
14) Generowania zestawienia wszystkich zasobów, w tym urządzeń i zainstalowanego na nich oprogramowania,
15) Przygotowania wielu szablonów generowanych dokumentów i protokołów przekazania zasobów wraz z konfigurowalną sekcją zawierającą dane i logo organizacji,
16) Konfiguracji stylu automatycznego numerowania dodawanych zasobów wg zdefiniowanego wzorca,
17) Konfiguracji stylu automatycznego numerowania dodawanych dokumentów i protokołów wg zdefiniowanego wzorca,
18) Archiwizacji i porównywania audytów zasobów,
19) Tworzenia kodów kreskowych dla zasobów,
20) Drukowania kodów kreskowych oraz dwuwymiarowych kodów alfanumerycznych (QR Code) dla zasobów, które posiadają numer inwentarzowy,
21) Inwentaryzacji zasobów posiadających kody kreskowe za pomocą aplikacji mobilnej dla systemu Android poprzez wyszukiwanie zasobów, skanowanie etykiet, dodawanie i edycję zasobów, dodawanie czynności serwisowych, drukowanie etykiet,
22) Inwentaryzacji stacji roboczych niepodłączonych do sieci (bez instalacji Agenta poprzez manualne wykonanie skanów inwentaryzacji offline),
23) Definiowania alarmów z powiadomieniami e-mail dla dowolnych pól czasowych typu „data" z atrybutów zasobów lub licencji (np. „za 2 tygodnie wygaśnie licencja/gwarancja");

Dodatkowo musi być dostępny również Agent inwentaryzacji na system Android.

Inwentaryzacja oprogramowania ma zapewniać funkcjonalność w zakresie pozyskiwania informacji o oprogramowaniu i audycie licencji poprzez:

1) Skanowanie plików wykonywalnych i multimedialnych na stacjach roboczych, skanowanie archiwów ZIP,
2) Informacje o aplikacjach używanych w organizacji,
3) Tworzenie własnych wzorców aplikacji,
4) Tworzenie dowolnych kategorii aplikacji, np. nowe, zabronione, projektowe itp.,
5) Informacje o komputerach, na których aplikacja została wykryta,
6) Zarządzanie posiadanymi licencjami,
7) Wskazywanie osób odpowiedzialnych za licencję,
8) Wskazanie użytkowników licencji,

9) Tworzenia powiązań między licencjami a dokumentami w relacji 1:N,
10) Rozbudowane zarządzanie licencjami poprzez: przypisywanie do użytkownika, przypisywanie do wielu komputerów tego samego użytkownika, przypisywanie wg numerów seryjnych, przypisywanie wg różnych wersji aplikacji na jednym urządzeniu,
11) Łatwy audyt legalności oprogramowania oraz powiadamianie tylko w razie przekroczenia liczby posiadanych licencji - w każdej chwili istnieje możliwość wykonania aktualnych raportów audytowych,
12) Zarządzanie posiadanymi licencjami: raport zgodności licencji,
13) Możliwość przypisania do programów numerów seryjnych, wartości itp.,

Okna audytowe mają posiadać możliwość filtrowania elementów per oddział.

3. Moduł do zarządzania użytkownikami:

Monitorowanie aktywności użytkowników pracujących na komputerach z systemem Windows poprzez monitorowanie:

1) Faktycznego czasu aktywności (dokładny czas pracy z godziną rozpoczęcia i zakończenia pracy),
2) Procesów (każdy proces ma całkowity czas działania oraz czas aktywności użytkownika) wraz informacją o uruchomieniu na podwyższonych uprawnieniach,
3) Rzeczywistego użytkowania programów (m.in. procentowa wartość wykorzystania aplikacji, obrazująca czas jej używania w stosunku do łącznego czasu, przez który aplikacja była uruchomiona) wraz z informacją, na którym komputerze wykonano daną aktywność,
4) Informacji o edytowanych przez użytkownika dokumentach,
5) Historii pracy (cykliczne zrzuty ekranowe),
6) Listy odwiedzanych stron WWW (liczba odwiedzin stron z nagłówkami, liczbą i czasem wizyt),
7) Transferu sieciowego użytkowników (ruch lokalny i transfer internetowy generowany przez użytkownika),
8) Wydruków m.in. informacje o dacie wydruku, informacje o wykorzystaniu drukarek, raporty dla każdego użytkownika (kiedy, ile stron, jakiej jakości, na jakiej drukarce, jaki dokument był drukowany), zestawienia pod względem stacji roboczej (kiedy, ile stron, jakiej jakości, na jakiej drukarce, jaki dokument drukowano z danej stacji roboczej), możliwość "grupowania" drukarek poprzez identyfikację drukarek. Program ma możliwość monitorowania kosztów wydruków,
9) Nagłówków przesyłanej w aplikacjach klienckich poczty e-mail;

Program ponadto musi mieć możliwość:

1) Blokowania stron internetowych poprzez możliwość zezwolenia lub zablokowania całego ruchu WWW dla stacji roboczej, na której zalogowany jest użytkownik, z możliwością definiowania wyjątków – zarówno zezwalających, jak i zabraniających korzystania z danych domen oraz wybranych lub dowolnych sub-domen (np. *.domena.pl). Reguły w postaci listy domen tworzone są dla użytkownika lub grupy użytkowników i mogą być kopiowane pomiędzy grupami lub kontami,
2) Blokowania ruchu na wskazanych portach TCP/IP,

3) Blokowania pobierania poprzez przeglądarki internetowe plików z określonym rozszerzeniem,
4) Wysyłania powiadomień gdy użytkownik: odwiedzi stronę z określonej grupy domeny; pobierze lub wyśle określoną ilość danych w ciągu dnia w sieci lokalnej lub Internet; wydrukuje określoną ilość stron w ciągu dnia,
5) Przygotowania zestawienia (metryki) ustawień monitorowania użytkownika w postaci raportu (który można dołączyć np. do akt pracownika),
6) Definiowania godzin lub dni tygodnia, w których monitorowanie użytkowników jest wyłączone,
7) Generowania raportów dla użytkowników Active Directory niezależnie od tego, na jakich komputerach pracowali w danym czasie,
8) Mechanizm blokowania uruchamiania aplikacji wg maski nazwy oraz lokalizacji pliku. Reguły w postaci listy blokowanych plików lub lokalizacji tworzone są dla użytkownika lub grupy użytkowników i mogą być kopiowane pomiędzy grupami lub kontami,
9) Program ma posiadać Grupy użytkowników oraz Grupy Inteligentne, które służą do lepszego zarządzania użytkownikami, polityką monitorowania oraz blokowania aplikacji i stron internetowych;

4. <u>Moduł zarządzania dostępem do danych i ich ochrony:</u>

1) Blokowanie urządzeń i nośników danych - możliwość zarządzania prawami dostępu do wszystkich urządzeń wejścia i wyjścia oraz urządzeń fizycznych, na które użytkownik może skopiować pliki z komputera urzędu lub uruchomić z nich program zewnętrzny,
2) Blokowanie urządzeń i interfejsów fizycznych: USB, FireWire, gniazda kart pamięci, SATA, dyski przenośne, napędy CD/DVD, stacje dyskietek,
3) Blokowanie interfejsów bezprzewodowych: Wi-Fi, Bluetooth, IrDA,
4) Blokownie dotyczy tylko urządzeń służących do przenoszenia danych - inne urządzenia (drukarka, klawiatura, mysz itp.) mogą być podłączane,
5) Alarmowanie o zdarzeniach podłączenia/odłączenia urządzeń zewnętrznych wraz z możliwością ograniczenia alarmów tylko do nośników niezaufanych,
6) Funkcje wspierające bezpieczeństwo systemu: monitorowanie stanu szyfrowania dysków BitLocker,
7) Funkcje wspierające bezpieczeństwo systemu: integracja z Windows Defender w zakresie odczytu stanu ochrony, włączenia i wyłączenia ochrony, tworzenia reguł ruchu,
8) Funkcje wspierające bezpieczeństwo systemu: monitorowanie stanu modułu TPM;
9) Zarządzanie prawami dostępu do urządzeń:
   a) definiowanie praw użytkowników/grup do odczytu, zapisu czy wykonania plików,
   b) autoryzowanie urządzeń firmowych (przykładowo szyfrowanych): pendrive'ów, dysków itp. – urządzenia prywatne są blokowane,
   c) całkowite zablokowanie określonych typów urządzeń dla wybranych użytkowników,
   d) centralna konfiguracja poprzez ustawienie reguł (polityk) dla całej sieci,

e) możliwość usuwania z listy znanych urządzeń tych nośników, które np. zostały zutylizowane;

10) Audyt operacji na plikach na urządzeniach przenośnych (zapisywanie informacji o zmianach w systemie plików na urządzeniach przenośnych, podłączenie/odłączenie urządzenia przenośnego,

11) Monitorowanie operacji na plikach w lokalnych folderach komputera użytkownika,

12) Integracja z Active Directory - zarządzanie prawami dostępu przypisanymi do użytkowników oraz grup domenowych,

13) Przydzielanie uprawnień również do kont użytkowników lokalnych;

.

Osoba od strony zamawiającego wyznaczona do kontaktu: Marcin Mróz tel. 46 874-62-94 wew. 20.

Ofertę prosimy przesłać pocztą lub złożyć osobiście w siedzibie Zamawiającego (Urząd Gminy Dmosin, Dmosin 9, 95 – 061 Dmosin , pok.), pocztą elektroniczną na adres: oferty@dmosin.pl w terminie do 05.08.2023 r.

Z up. Wójta
Jolanta Wojciechowska
Sekretarz Gminy

Dmosin, dnia 25.07.2023

.....
(podpis osoby prowadzącej postępowanie)