POWIAT [illegible]
[illegible]
ul. Ko[illegible] 28
NIP [illegible]
REGON [illegible]

SZP.033.5.2.2026 Kozienice, dnia 09.03.2026 r.

- Wykonawcy biorący udział w postępowaniu -

dotyczy zaproszenia do złożenia propozycji cenowej na zadanie pod nazwą: „Dzierżawa wielofunkcyjnych urządzeń drukująco – kopiujących wraz z ich kompleksową obsługą serwisową na potrzeby Starostwa Powiatowego w Kozienicach" /SZP.033.5.2026/ z dnia 03.03.2026 r.

Pytania i Odpowiedzi Nr 1 (pytania z dnia 06.03.2026 r.)

Pytanie 1
W nawiązaniu do postępowania: „Dzierżawa wielofunkcyjnych urządzeń drukująco – kopiujących wraz z ich kompleksową obsługą serwisową na potrzeby Starostwa Powiatowego w Kozienicach" /SZP.033.5.2026/ - proszę o dopuszczenie Wykonawcy oferującego urządzenia:

Urządzenie Typ I – wielofunkcyjne, kolorowe formatu A3, 3 sztuki:

- czas uruchomienia: 13 s
- format zapisywanych plików: TIFF, JPEG, PDF, XPS, skompresowany PDF, PDF/A-1b, przeszukiwalny PDF/XPS, Office Open XML (PowerPoint, Word)
- wydajność tonerów 28 000 kopii- czy zamawiający dopuści równoważną ilość tonerów na 70 tys. wydruków mono i 60 tys. wydruków kolor?
- wydajność bębnów: K= 240 000 wydruków, CMYK = 165 000 wydruków
- zabezpieczenie dokumentu- wskazuje w postępowaniu przetargowym tylko na producenta: CANON co jest nie zgodne z zasadą konkurencyjności.
- Bezpieczne drukowanie, integracja zarządzania prawami Adobe LiveCycle Rights Management? ES2.5, szyfrowane pliki PDF, szyfrowane bezpieczne drukowanie, podpis urządzenia, zabezpieczające znaki wodne.

ODPOWIEDŹ: Zamawiający dopuszcza zmianę w zakresie: czas uruchomienia 13 s, format zapisywanych plików: TIFF, JPEG, PDF, XPS, skompresowany PDF, PDF/A-1b, przeszukiwalny PDF/XPS, Office Open XML (PowerPoint, Word)
Bezpieczne drukowanie, szyfrowane pliki PDF, szyfrowane bezpieczne drukowanie, podpis urządzenia, zabezpieczające znaki wodne.
Zamawiający nie dopuszcza zmiany w zakresie wydajności tonerów i bębnów ze względu na miejsce i charakter pracy urządzenia. Przewidywanie natężenie pracy wymagałoby częstszej interwencji operatora w przypadku niższych wydajności.

Wnosimy o wykreślenie tego zapisu

- zabezpieczenie urządzenia:

Wnosimy o zmianę zapisów, które w obecnej formie prowadzą do faktycznego uprzywilejowania jednego producenta – marki Canon, ograniczając tym samym zasadę uczciwej konkurencji. Uwzględnienie rozwiązań alternatywnych pozwoli na rozszerzenie grona oferentów, podniesienie poziomu bezpieczeństwa urządzeń oraz uzyskanie korzystniejszych warunków realizacji zamówienia.

Dotyczy parametru "Zabezpieczenia urządzenia":
Było: "Ochrona danych na dysku SSD (szyfrowanie danych na dysku SSD, blokada dysku SSD), standardowa inicjalizacja dysku SSD, moduł TPM 2.0, funkcja ukrywania dziennika zadań, ochrona integralności oprogramowania MFD, sprawdzanie integralności oprogramowania MFD i odporności oprogramowania układowego platformy (NIST SP800-193) z automatycznym odzyskiwaniem systemu (weryfikacja systemu przy uruchomieniu, wykrywanie włamań w czasie pracy dzięki oprogramowaniu McAfee Embedded Control), certyfikat Common Criteria HCD-PP"
Zwracamy się z prośbą o zmianę na: "Ochrona danych na dysku SSD (szyfrowanie danych na dysku SSD, blokada dysku SSD), standardowa inicjalizacja dysku SSD, moduł TPM, funkcja ukrywania dziennika zadań, weryfikacja integralności oprogramowania oraz funkcja wykrywania włamań, skanowanie plików i połączeń sieciowych w czasie pracy dzięki oprogramowaniu McAfee Embedded Control lub oprogramowania antywirusowego innego producenta, certyfikat Common Criteria ISO 15408 HCD-PP, powiadomienia o incydentach bezpieczeństwa, Secure Erase.

ODPOWIEDŹ: Zamawiający dopuszcza zmianę w ww. zakresie. Ochrona danych na dysku SSD (szyfrowanie danych na dysku SSD, blokada dysku SSD), standardowa inicjalizacja dysku SSD, moduł TPM 2.0, funkcja ukrywania dziennika zadań, ochrona integralności oprogramowania MFD, sprawdzanie integralności oprogramowania MFD i odporności oprogramowania układowego platformy (NIST SP800-193) z automatycznym odzyskiwaniem systemu (weryfikacja systemu przy uruchomieniu, wykrywanie włamań w czasie pracy dzięki oprogramowaniu McAfee Embedded Control lub oprogramowania antywirusowego innego producenta), certyfikat Common Criteria HCD-PP.

1. moduł TPM 2.0:

Pozostawienie wymogu zastosowania wyłącznie modułu TPM w wersji 2.0 prowadzi do nieuzasadnionego ograniczenia konkurencji i zawężenia kręgu potencjalnych wykonawców. Z punktu widzenia Zamawiającego kluczowe znaczenie ma funkcjonalność i poziom bezpieczeństwa, a nie sztywne wskazanie wersji modułu.
Moduł TPM – niezależnie od wersji – zapewnia sprzętową ochronę kluczy kryptograficznych oraz bezpieczne operacje szyfrowania i deszyfrowania danych przechowywanych na urządzeniu. W szczególności szyfrowanie danych przy użyciu klucza 256-bitowego (np. AES-256) stanowi powszechnie uznany i zatwierdzony przez NIST standard bezpieczeństwa, szeroko stosowany do ochrony danych wrażliwych.
Rezygnacja z narzucenia konkretnej wersji TPM, przy jednoczesnym zachowaniu wymaganego poziomu bezpieczeństwa, zwiększy konkurencyjność postępowania i umożliwi udział większej liczbie wykonawców, bez jakiegokolwiek uszczerbku dla interesów Zamawiającego.

ODPOWIEDŹ: Zamawiający nie zamierza dokonać modyfikacji w ww. zakresie. Moduł TPM 2.0: Wymagany przez Microsoft od lipca 2016 roli. Pierwsze urządzenia pojawiły się w 2014 roku. Na rynku istnieją modele kilku producentów spełniające te wymagania, zapis ten więc nie narusza zasady uczciwej konkurencji.

2. Ochrona integralności oprogramowania MFD, sprawdzanie integralności oprogramowania MFD i odporności oprogramowania układowego platformy (NIST SP800-193) z automatycznym odzyskiwaniem systemu (weryfikacja systemu przy uruchomieniu, wykrywanie włamań w czasie pracy dzięki oprogramowaniu McAfee Embedded Control)

Aktualny zapis łączy w jednym wymaganiu:
- określony standard (NIST SP 800-193),
- konkretne mechanizmy techniczne,
- oraz wskazanie konkretnego komercyjnego rozwiązania (McAfee Embedded Control).

Takie zestawienie prowadzi w praktyce do uprzywilejowania producenta, a w konsekwencji do ograniczenia zasady uczciwej konkurencji i neutralności technologicznej.
Celem wytycznych NIST SP 800-193 jest zapewnienie odporności platformy sprzętowej i oprogramowania układowego (firmware) na: nieautoryzowane modyfikacje, trwałe ataki na integralność systemu oraz umożliwienie bezpiecznego odzyskiwania systemu.
Cele te mogą zostać osiągnięte zaproponowanymi, równoważnymi środkami technicznymi, takimi jak:
- weryfikacja integralności firmware podczas uruchamiania,
- wykrywanie prób naruszenia integralności systemu na poziomie firmware lub systemowym,
- bezpieczne mechanizmy kasowania danych (Secure Erase zgodne z wytycznymi NIST),
- zastosowanie oprogramowania antywirusowego lub mechanizmów ochronnych innych producentów, zapewniających równoważny poziom bezpieczeństwa.

Wymaganie zastosowania konkretnego produktu McAfee Embedded Control, zamiast opisania wymaganej funkcji bezpieczeństwa, stanowi odwołanie do określonego rozwiązania komercyjnego, a nie do efektu, jaki Zamawiający chce osiągnąć. Może to być postrzegane jako naruszenie zasady neutralności technologicznej.

ODPOWIEDŹ: Zamawiający dopuszcza zmianę w ww. zakresie. „...ochrona integralności oprogramowania MFD, sprawdzanie integralności oprogramowania MFD i odporności oprogramowania układowego platformy (NIST SP800-193) z automatycznym odzyskiwaniem systemu (weryfikacja systemu przy uruchomieniu, wykrywanie włamań w czasie pracy dzięki oprogramowaniu McAfee Embedded Control lub rozwiązania równoważnego)"

Dotyczy parametru: „Zabezpieczenia sieciowe":

Było: TLS 1.3, IPSec, uwierzytelnianie IEEE 802.1X, obsługa protokołu WPA3, SNMP v3.0, funkcje zapory sieciowej (filtrowanie adresów IP/MAC), obsługa dwóch sieci (przewodowa sieć LAN / bezprzewodowa sieć LAN, przewodowa sieć LAN / przewodowa sieć LAN), wyłączanie nieużywanych funkcji (włączanie/wyłączanie protokołów/aplikacji, włączanie/wyłączanie zdalnego interfejsu użytkownika, włączanie/wyłączanie interfejsu USB), rozdzielenie linii komunikacyjnej (G3, port USB, zaawansowana przestrzeń, skanowanie i wysyłanie wiadomości e-mail z ostrzeżeniem o wirusach).

Zwracamy się z prośbą o zmianę na: TLS 1.3, IPSec, uwierzytelnianie IEEE 802.1X, obsługa protokołu WPA3, SNMP v3.0, funkcje zapory sieciowej (filtrowanie adresów IP/MAC), obsługa dwóch sieci (przewodowa sieć LAN / bezprzewodowa sieć WLAN), wyłączanie nieużywanych funkcji (włączanie/wyłączanie protokołów i aplikacji, włączanie/wyłączanie zdalnego interfejsu użytkownika, włączanie/wyłączanie interfejsu USB), oddzielna obsługa sieci analogowej i internetowej (w tym obsługa modułu faksu G3 – o ile wymagany), wysyłanie wiadomości e-mail z ostrzeżeniami o zagrożeniach (np. wykrycie wirusa).

ODPOWIEDŹ: Zamawiający dopuszcza zmianę w ww. zakresie. TLS 1.3, IPSec, uwierzytelnianie IEEE 802.1X, obsługa protokołu WPA3, SNMP v3.0, funkcje zapory sieciowej (filtrowanie adresów IP/MAC), obsługa dwóch sieci (przewodowa sieć LAN / bezprzewodowa sieć LAN lub przewodowa sieć LAN / przewodowa sieć LAN), wyłączanie nieużywanych funkcji (włączanie/wyłączanie protokołów/aplikacji, włączanie/wyłączanie zdalnego interfejsu użytkownika, włączanie/wyłączanie interfejsu USB), zaawansowana przestrzeń, skanowanie i wysyłanie wiadomości e mail z ostrzeżeniem o wirusach).

Uzasadnienie proponowanych zmian:

1. Obsługa dwóch sieci (LAN/LAN vs LAN/WLAN):

Aktualny zapis wymaga obsługi dwóch w pełni oddzielonych przewodowych interfejsów LAN (LAN/LAN). Takie rozwiązanie występuje wyłącznie w ograniczonej liczbie urządzeń i jest charakterystyczne dla określonych producentów.

Tymczasem zdecydowana większość urządzeń MFP dostępnych na rynku realizuje separację dwóch sieci poprzez konfigurację LAN/WLAN, która zapewnia równoważny poziom bezpieczeństwa.

Z perspektywy bezpieczeństwa teleinformatycznego istotny jest efekt końcowy w postaci separacji sieci, a nie konkretna forma fizycznej implementacji. Narzucenie wyłącznie konfiguracji LAN/LAN, bez dopuszczenia równoważnej konfiguracji LAN/WLAN, jest nieproporcjonalne do celu i prowadzi do nieuzasadnionego wykluczenia producentów stosujących powszechnie akceptowane rozwiązania.

Dopuszczenie zapisu „obsługa dwóch sieci (np. LAN/WLAN)" zwiększy konkurencyjność postępowania, przy jednoczesnym zachowaniu wymaganej separacji i poziomu bezpieczeństwa.

ODPOWIEDŹ: Zamawiający dopuszcza zmianę zapisu na „obsługa dwóch sieci (np. LAN/LAN lub LAN/WLAN)"

2. Rozdzielenie linii komunikacyjnych:

Obecny wymóg rozdzielenia linii komunikacyjnej poprzez zestaw elementów opisanych jako: „G3, port USB, zaawansowana przestrzeń, skanowanie i wysyłanie wiadomości e-mail z ostrzeżeniem o wirusach" jest skonstruowany w sposób odpowiadający konkretnej architekturze jednego producenta.

W praktyce większość urządzeń MFP osiąga ten sam poziom bezpieczeństwa poprzez:

- logiczne oddzielenie obsługi sieci analogowej (np. faks G3) od sieci IP,
- możliwość blokowania lub fizycznego wyłączania interfejsów USB,
- skanowanie przesyłanych plików i generowanie alertów bezpieczeństwa z poziomu firmware lub modułu ochronnego.

Osiągnięcie celu bezpieczeństwa nie wymaga narzucania konkretnego modelu architektonicznego ani sposobu implementacji. Proponowany zapis koncentruje się na efekcie bezpieczeństwa, a nie na wymuszaniu specyficznej konstrukcji sprzętowej lub programowej, co jest zgodne z zasadą neutralności technologicznej.

ODPOWIEDŹ: Zamawiający dopuszcza zmianę zapisu w ww. zakresie.

3. Doprecyzowanie wymogu dotyczącego faksu G3:

Zwracamy się z prośbą o jednoznaczne doprecyzowanie, czy Zamawiający wymaga, aby oferowane urządzenia były obowiązkowo wyposażone w moduł faksu G3.

W pozostałych częściach specyfikacji nie wskazano wprost takiego wymogu. Jedyną przesłanką sugerującą jego istnienie jest użycie oznaczenia „G3" w zapisie dotyczącym rozdzielenia linii komunikacyjnych. Prosimy o potwierdzenie, czy:

- faks G3 jest funkcjonalnością obligatoryjną,
- czy też zapis ten odnosi się wyłącznie do ogólnej zasady separacji kanałów komunikacyjnych – o ile taka funkcja występuje w urządzeniu.

Doprecyzowanie tego punktu pozwoli uniknąć rozbieżnych interpretacji i ułatwi przygotowanie porównywalnych ofert.

Odpowiedź: Zamawiający nie wymaga, aby oferowane urządzenia były wyposażone w moduł faksu G3.

Podsumowanie:

Dopuszczenie rozwiązań równoważnych, przy jednoczesnym utrzymaniu wysokich wymagań w zakresie bezpieczeństwa sieciowego, pozwoli Zamawiającemu:

- osiągnąć zakładany poziom ochrony danych i komunikacji,
- zwiększyć liczbę potencjalnych oferentów,
- wzmocnić konkurencyjność postępowania,
- oraz uzyskać korzystniejsze warunki ekonomiczne realizacji zamówienia.

Proponowane zmiany nie obniżają poziomu bezpieczeństwa, lecz zapewniają jego realizację w sposób proporcjonalny, neutralny technologicznie i zgodny z zasadami uczciwej konkurencji.

Urządzenie Typ II – monochromatyczne urządzenie wielofunkcyjne A3 - 1 sztuka:
- czas uruchomienia: 12 s
- pojemność tac odbiorczych: 2200 arkuszy
- Funkcje wykańczania:

Sortowanie, grupowanie, układanie z przesunięciem, zszywanie, broszurowanie, zszywanie na żądanie
- szafka pod urządzenie: nie może być szafki bo są kasety na dużą ilość papieru jaką Zamawiający wymaga
- wydajność tonera 28 000 kopii- czy zamawiający dopuści równoważną ilość tonerów na 44 tys. mono

ODPOWIEDŹ: Zamawiający dopuszcza zmianę w zakresie czasu uruchomienia urządzenia: 12 s.
Zamawiający, wymagając szafkę pod urządzenie, miał na myśli dodatkowe kasety na papier z kółkami.
Zamawiający nie dopuszcza zmiany w zakresie pojemności tac odbiorczych, funkcji wykańczania i wydajności tonerów, ze względu na miejsce i charakter pracy urządzenia. Przewidywanie natężenie pracy wymagałoby częstszej interwencji operatora w przypadku niższych parametrów tych funkcji.

Urządzenie Typ III – monochromatyczne urządzenie wielofunkcyjne A3 - 3 sztuki
- czas uruchomienia: 12 s
- wydajność tonera 28 000 kopii- czy zamawiający dopuści równoważną ilość tonerów na 44 tys. mono

Urządzenie Typ IV – monochromatyczne urządzenie wielofunkcyjne A4- 3 sztuki
- prędkość druku A4: 47 str. A4/min
- czas uruchomienia: 13 s
- pojemność papieru: 600 arkuszy
- funkcje wykańczania: bez zastosowania tej opcji
- pojemność podajnika papieru: 80 arkuszy
- prędkość skanowania: 1 str.: 45, 2 str.: 90
- wydajność tonera 20 000 kopii- czy zamawiający dopuści równoważną ilość tonerów na 51 tys. mono

ODPOWIEDŹ: Zamawiający dopuszcza zmianę w zakresie czasu uruchomienia urządzenia: 13 s., pojemność podajnika papieru: 80 arkuszy.
Zamawiający nie dopuszcza zmiany w zakresie prędkości druku, pojemności papieru, funkcji wykańczania, prędkości skanowania i wydajności tonera, ze względu na miejsce i charakter pracy urządzenia. Przewidywanie natężenie pracy wymagałoby częstszej interwencji operatora w przypadku niższych parametrów.

Dopuszczenie rozwiązań równoważnych jest konieczne, ponieważ wskazanie konkretnych producentów lub nazw handlowych narusza zasadę neutralności technologicznej, podczas gdy identyczny efekt bezpieczeństwa może być osiągnięty również przy użyciu funkcji takich jak szyfrowany dysk SSD, weryfikacja integralności oprogramowania czy zaawansowana ochrona antywirusowa, w tym Bitdefender dostępny w urządzeniach Wykonawcy. Urządzenia te spełniają wymagania dotyczące szyfrowania PDF/A, podpisów cyfrowych, znaków wodnych oraz kontroli uprawnień dokumentu, co zapewnia pełną równoważność funkcjonalną bez konieczności stosowania Adobe LiveCycle wskazanego w OPZ. W zakresie sieci i komunikacji zapewniają obsługę TLS/SSL, IPsec, 802.1X oraz separację sieci poprzez VLAN lub tryby Wired + Wireless, co realizuje ten sam cel bezpieczeństwa bez ograniczania postępowania do urządzeń z podwójnym fizycznym interfejsem LAN/LAN. Ponadto i-Series oferują certyfikowane mechanizmy bezpieczeństwa zgodne z Common Criteria ISO/IEC 15408 (HCD-PP) lub równoważne rozwiązania implementujące wymagane funkcje ochrony, co potwierdza ich zgodność z wysokimi standardami bezpieczeństwa oczekiwanymi w sektorze publicznym. Wymagane w OPZ parametry materiałów eksploatacyjnych mogą być spełnione poprzez dostarczenie równoważnej łącznej wydajności tonerów, co jest zgodne z ISO i pozostaje praktyką powszechnie akceptowaną w zamówieniach publicznych, szczególnie przy wydajnościach tonerów rzędu 20–28 tys. stron dla modeli Wykonawcy.
Dopuszczenie rozwiązań równoważnych zwiększy konkurencyjność postępowania, obniży koszty zakupu, a Zamawiający uzyska urządzenia o potwierdzonych, wysokich standardach bezpieczeństwa i funkcjonalności, w pełni odpowiadających wymaganiom OPZ

Zamawiający informuje, iż wymaga dostarczenia urządzeń Wykonawcy, ich instalacji i konfiguracji oraz objęcie urządzeń systemem do monitorowania ich stanu pracy w terminie pozwalającym na rozpoczęcie korzystania z przedmiotu zamówienia najpóźniej **od dnia 16.03.2026 r.** Dostarczenie urządzeń, ich instalacja i konfiguracja oraz objęcie dostarczonych urządzeń systemem do monitorowania ich stanu pracy, powinno nastąpić przed dniem

rozpoczęcia usługi Obsługi Wydruku. Oznacza to, że **w dniu 16.03.2026 r.** Zamawiający będzie miał pełną możliwość korzystania ze wszystkich opisanych parametrów Obsługi Wydruku (tj. drukowania, kopiowania i skanowania dokumentów na wszystkich dostarczonych urządzeniach Wykonawcy po uprzednim przeszkoleniu, oraz posiada możliwość korzystania z obsługi serwisowej).
Za termin realizacji zamówienia uważa się okres 36 miesięcy liczonych od daty protokolarnej dostawy i uruchomienia w siedzibie Zamawiającego przedmiotu zamówienia nie później jednak niż **od dnia 16 marca 2026 r.**

Zamawiający informuje, że powyższe pytania oraz odpowiedzi na nie stają się integralną częścią przedmiotu zamówienia i będą wiążące podczas składania ofert (należy je uwzględnić składając ofertę w ramach przedmiotowego postępowania).

Mając na uwadze powyższe Zamawiający informuje, iż wydłuża termin składania ofert do dnia 11.03.2026 roku do godziny 10:00.

POWIAT [illegible]
[illegible]
ul. [illegible]
NIP [illegible]
REGON 670223155

STAROSTA
mgr Krzysztof Wolski