Włoszczowa dn 2.12.2019r.

AG.2600.6.2019.I

ZAPYTANIE OFERTOWE

ZAMAWIAJĄCY: Powiat Włoszczowski - Starostwo Powiatowe we Włoszczowie ul. Wiśniowa 10, 29-100 Włoszczowa,
zaprasza do złożenia oferty w postępowaniu dotyczącym udzielenia zamówienia, którego wartość nie przekracza wyrażonej w złotych równowartości kwoty określonej w art. 4 pkt 8 ustawy z dnia 29 stycznia 2004 r. Prawo zamówień publicznych na:

Kompleksową obsługę serwisową wraz z dzierżawą urządzeń drukujących, kopiujących, dostawę materiałów eksploatacyjnych i zabezpieczeniem sieci.

OPIS PRZEDMIOTU ZAMÓWIENIA

I. **Przedmiotem zamówienia** jest świadczenie usługi dzierżawy urządzeń wielofunkcyjnych dla Starostwa Powiatowego we Włoszczowie oraz urządzenia do zabezpieczenia sieci - UTM. Na przedmiot zamówienia muszą składać się następujące usługi:
   - transport, montaż i uruchomienie wszystkich urządzeń,
   - serwis, w tym konserwacja i bieżące naprawy urządzeń, dostarczanie materiałów eksploatacyjnych (w szczególności: bębny, tonery, wymiana zużytych części) urządzeń dzierżawionych,
   - dostarczanie materiałów eksploatacyjnych dla urządzeń posiadanych przez Zamawiającego,
   - w przypadku awarii urządzenia dostarczenie zastępczego urządzenia o nie gorszych parametrach technicznych niż urządzeń, które uległo awarii,

II. **Liczba urządzeń**:

- Laserowe urządzenie wielofunkcyjne A3/A4 z terminalem do autoryzacji: 3 urządzenia **z czego przynajmniej jedno musi być fabrycznie nowe**;
- Drukarka monochromatyczna A4 – 27 **urządzeń fabrycznie nowych**;
- UTM – 1 urządzenie, fabrycznie nowe z licencją przynajmniej na rok;

Każde urządzenie wielofunkcyjne winno drukować po uprzedniej autoryzacji przez użytkownika za pomocą indywidualnego kodu PIN.

III. Dane techniczne urządzeń:

1. Laserowe urządzenie wielofunkcyjne A3/A4 z terminalem do autoryzacji A3 mono/kolor

Lp.	Nazwa komponentu	Wymagane minimalne parametry techniczne
1	2	3
1	prędkość kopiowania w czerni i kolorze	25str./min. A4, 15str./min. A3
2	technologia powielania	laserowa w kolorze
3	panel	Uchylny, dotykowy LCD o przekątnej 9"
4	format oryginału i kopii	A5R-A3; 52-280 g/m²
5	zoom	25% - 400%
6	czas nagrzewania z trybu uśpienia	12 sekund
7	kody dostępu	1 000
8	pojemność pamięci	2 GB RAM
9	twardy dysk	dysk twardy o pojemności 160GB
10	rozdzielczość druku	600x1200 dpi
11	gramatura papieru	52 - 280 g/m²
12	Kasety	2 x kaseta na papier po 550 arkuszy każda (80 g/m²);
13	Podajnik ręczny	podajnik ręczny: 100 arkuszy
14	Podajnik dokumentów	dwustronny o pojemności 100 arkuszy (80g/m²)
15	skanowanie	szybkość skanowania w kolorze73 obrazy/min
16	Wydajność tonerów	- Tonerów, umożliwiający wydrukowanie min. 33 000 wydruków przy pokryciu strony w 5%.

2. **Drukarka monochromatyczna A4**

Nazwa parametru	Wymagania minimalne
Technologia druku	Laserowa

Rodzaj druku	Monochromatyczny
Rozdzielczość	1200 X 1200 dpi
Format wydruku	A4
Prędkość druku	45 stron A4/minutę
Pamięć RAM	64 MB
Emulacje	PCL 6, PCL 5e, PostScriptslub emulacja
Interfejsy	USB 2.0, Gigabit Ethernet 10/100 BaseT
Obsługiwane systemy operacyjne	Windows Vista/7/8/10
Podajniki papieru	1 podajnik w formie zamkniętej kasety na minimum 500 arkuszy A4 80 g/m^2, 1 podajnik wielofunkcyjny na minimum 50 arkuszy A4 80 g/m^2.
Odbiornik papieru	Na min. 250 arkuszy A4 80 g/m^2
Wydruk dwustronny	Automatyczny
Materiały Eksploatacyjne	Drukarka musi obsługiwać standardowy toner na min.10000 str.
Stan techniczny	Fabrycznie nowa

3. UTM

Wymagania Ogólne

Dostarczony system bezpieczeństwa musi zapewniać wszystkie wymienione poniżej funkcje sieciowe i bezpieczeństwa niezależnie od dostawcy łącza. Dopuszcza się aby poszczególne elementy wchodzące w skład systemu bezpieczeństwa były zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub komercyjnych aplikacji instalowanych na platformach ogólnego przeznaczenia. W przypadku implementacji programowej dostawca musi zapewnić niezbędne platformy sprzętowe wraz z odpowiednio zabezpieczonym systemem operacyjnym.

System realizujący funkcję Firewall musi dawać możliwość pracy w jednym z trzech trybów: Routera z funkcją NAT, transparentnym oraz monitorowania na porcie SPAN.

W ramach dostarczonego systemu bezpieczeństwa musi być zapewniona możliwość budowy minimum 2 oddzielnych (fizycznych lub logicznych) instancji systemów w zakresie: Routingu, Firewall'a, IPSec VPN, Antywirus, IPS, Kontroli Aplikacji. Powinna istnieć możliwość dedykowania co najmniej 10 administratorów do poszczególnych instancji systemu.

System musi wspierać IPv4 oraz IPv6 w zakresie:

- Firewall.
- Ochrony w warstwie aplikacji.
- Protokołów routingu dynamicznego.

Redundancja, monitoring i wykrywanie awarii

1) W przypadku systemu pełniącego funkcje: Firewall, IPSec, Kontrola Aplikacji oraz IPS – musi istnieć możliwość łączenia w klaster Active-Active lub Active-Passive. W obu trybach powinna istnieć funkcja synchronizacji sesji firewall.
2) Monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łączy sieciowych.
3) Monitoring stanu realizowanych połączeń VPN.
4) System musi umożliwiać agregację linków statyczną oraz w oparciu o protokół LACP. Powinna istnieć możliwość tworzenia interfejsów redundantnych.

Interfejsy, Dysk, Zasilanie:

1) System realizujący funkcję Firewall musi dysponować minimum:
   - 20 portami Gigabit Ethernet RJ-45.
   - 2 gniazdami SFP 1 Gbps.
2) System Firewall musi posiadać wbudowany port konsoli szeregowej oraz gniazdo USB umożliwiające podłączenie modemu 3G/4G oraz instalacji oprogramowania z klucza USB.
3) W ramach systemu Firewall powinna być możliwość zdefiniowania co najmniej 200 interfejsów wirtualnych - definiowanych jako VLAN'y w oparciu o standard 802.1Q.
4) System musi być wyposażony w zasilanie AC.

Parametry wydajnościowe:

1) W zakresie Firewall'a obsługa nie mniej niż 2 mln jednoczesnych połączeń oraz 30.000 nowych połączeń na sekundę.
2) Przepustowość Stateful Firewall: nie mniej niż 7.4 Gbps.
3) Przepustowość Firewall z włączoną funkcją Kontroli Aplikacji: nie mniej niż 1 Gbps.
4) Wydajność szyfrowania IPSec VPN: nie mniej niż 4 Gbps.
5) 7. Wydajność skanowania ruchu w celu ochrony przed atakami (zarówno clientside jak i serverside w ramach modułu IPS) dla ruchu Enterprise Traffic Mix - minimum 500 Mbps.
6) 8. Wydajność skanowania ruchu typu Enterprise Mix z włączonymi funkcjami: IPS, Application Control, Antywirus - minimum 250 Mbps.
7) 9. Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL dla ruchu http – minimum 130 Mbps.

Funkcje Systemu Bezpieczeństwa:

W ramach dostarczonego systemu ochrony muszą być realizowane wszystkie poniższe funkcje. Mogą one być zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub programowych:

1) Kontrola dostępu - zapora ogniowa klasy StatefulInspection.
2) Kontrola Aplikacji.
3) Poufność transmisji danych - połączenia szyfrowane IPSec VPN oraz SSL VPN.
4) Ochrona przed malware – co najmniej dla protokołów SMTP, POP3, IMAP, HTTP, FTP, HTTPS.
5) Ochrona przed atakami - IntrusionPrevention System.
6) Kontrola stron WWW.

7) Kontrola zawartości poczty – Antyspam dla protokołów SMTP, POP3.
8) Zarządzanie pasmem (QoS, Trafficshaping).
9) Mechanizmy ochrony przed wyciekiem poufnej informacji (DLP).
10) Dwu-składnikowe uwierzytelnianie z wykorzystaniem tokenów sprzętowych lub programowych. W ramach postępowania powinny zostać dostarczone co najmniej 2 tokeny sprzętowe lub programowe, które będą zastosowane do dwu-składnikowego uwierzytelnienia administratorów lub w ramach połączeń VPN typu client-to-site.
11) Analiza ruchu szyfrowanego protokołem SSL.
12) Analiza ruchu szyfrowanego protokołem SSH.

Polityki, Firewall

1) System Firewall musi umożliwiać tworzenie list kontroli dostępu realizowanych bezstanowo przed funkcją FW.
2) Polityka Firewall musi uwzględniać adresy IP, użytkowników, protokoły, usługi sieciowe, aplikacje lub zbiory aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń.
3) System musi zapewniać translację adresów NAT: źródłowego i docelowego, translację PAT oraz:
   - Translację jeden do jeden oraz jeden do wielu.
   - Dedykowany ALG (Application Level Gateway) dla protokołu SIP.
4) W ramach systemu musi istnieć możliwość tworzenia wydzielonych stref bezpieczeństwa np. DMZ, LAN, WAN.

Połączenia VPN

1) System musi umożliwiać konfigurację połączeń typu IPSec VPN. W zakresie tej funkcji musi zapewniać:
   - Wsparcie dla IKE v1 oraz v2.
   - Obsługa szyfrowania protokołem AES z kluczem 128 i 256 bitów w trybie pracy Galois/CounterMode(GCM).
   - Obsługa protokołu Diffie-Hellman grup 19 i 20.
   - Wsparcie dla Pracy w topologii Hub and Spoke oraz Mesh, w tym wsparcie dla dynamicznego zestawiania tuneli pomiędzy SPOKE w topologii HUB and SPOKE.
   - Tworzenie połączeń typu Site-to-Site oraz Client-to-Site.
   - Monitorowanie stanu tuneli VPN i stałego utrzymywania ich aktywności.
   - Możliwość wyboru tunelu przez protokoły: dynamicznego routingu (np. OSPF) oraz routingu statycznego.
   - Obsługa mechanizmów: IPSec NAT Traversal, DPD, Xauth.
   - Mechanizm „Split tunneling" dla połączeń Client-to-Site.
2) System musi umożliwiać konfigurację połączeń typu SSL VPN. W zakresie tej funkcji musi zapewniać:
   - Pracę w trybie Portal - gdzie dostęp do chronionych zasobów realizowany jest za pośrednictwem przeglądarki. W tym zakresie system musi zapewniać stronę komunikacyjną działającą w oparciu o HTML 5.0.
   - Pracę w trybie Tunnel z możliwością włączenia funkcji „Split tunneling" przy zastosowaniu dedykowanego klienta.

Routing i obsługa łączy WAN

1) W zakresie routingu rozwiązanie powinno zapewniać obsługę:
   - Routingu statycznego.
   - Policy Based Routingu.
   - Protokołów dynamicznego routingu w oparciu o protokoły: RIPv2, OSPF, BGP oraz PIM.
2) System musi umożliwiać obsługę kilku (co najmniej dwóch) łączy WAN z mechanizmami statycznego lub dynamicznego podziału obciążenia oraz monitorowaniem stanu połączeń WAN.

Zarządzanie pasmem

1) System Firewall musi umożliwiać zarządzanie pasmem poprzez określenie: maksymalnej, gwarantowanej ilości pasma, oznaczanie DSCP oraz wskazanie priorytetu ruchu.
2) Musi istnieć możliwość określania pasma dla poszczególnych aplikacji.
3) System musi zapewniać możliwość zarządzania pasmem dla wybranych kategorii URL.

Kontrola Antywirusowa

1) Silnik antywirusowy musi umożliwiać skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021).
2) System musi umożliwiać skanowanie archiwów, w tym co najmniej: zip, RAR.
3) System musi dysponować sygnaturami do ochrony urządzeń mobilnych (co najmniej dla systemu operacyjnego Android).
4) System musi współpracować z dedykowaną platformą typu Sandbox lub usługą typu Sandbox realizowaną w chmurze. W ramach postępowania musi zostać dostarczona platforma typu Sandbox wraz z niezbędnymi serwisami lub licencja upoważniająca do korzystania z usługi typu Sandbox w chmurze.

Ochrona przed atakami

1) Ochrona IPS powinna opierać się co najmniej na analizie sygnaturowej oraz na analizie anomalii w protokołach sieciowych.
2) System powinien chronić przed atakami na aplikacje pracujące na niestandardowych portach.
3) Baza sygnatur ataków powinna zawierać minimum 6500 wpisów i być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.
4) Administrator systemu musi mieć możliwość definiowania własnych wyjątków oraz własnych sygnatur.
5) System musi zapewniać wykrywanie anomalii protokołów i ruchu sieciowego, realizując tym samym podstawową ochronę przed atakami typu DoS oraz DDoS.
6) Mechanizmy ochrony dla aplikacji Web'owych na poziomie sygnaturowym (co najmniej ochrona przed: CSS, SQL Injecton, Trojany, Exploity, Roboty) oraz możliwość kontrolowania długości nagłówka, ilości parametrów URL, Cookies.
7) Wykrywanie i blokowanie komunikacji C&C do sieci botnet.

Kontrola aplikacji

1) Funkcja Kontroli Aplikacji powinna umożliwiać kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP.
2) Baza Kontroli Aplikacji powinna zawierać minimum 2500 sygnatur i być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.
3) Aplikacje chmurowe (co najmniej: Facebook, Google Docs, Dropbox) powinny być kontrolowane pod względem wykonywanych czynności, np.: pobieranie, wysyłanie plików.
4) Baza powinna zawierać kategorie aplikacji szczególnie istotne z punktu widzenia bezpieczeństwa: proxy, P2P.
5) Administrator systemu musi mieć możliwość definiowania wyjątków oraz własnych sygnatur.

Kontrola WWW

1) Moduł kontroli WWW musi korzystać z bazy zawierającej co najmniej 40 milionów adresów URL pogrupowanych w kategorie tematyczne.
2) W ramach filtra www powinny być dostępne kategorie istotne z punktu widzenia bezpieczeństwa, jak: malware (lub inne będące źródłem złośliwego oprogramowania), phishing, spam, Dynamic DNS, proxy.
3) Filtr WWW musi dostarczać kategorii stron zabronionych prawem: Hazard.
4) Administrator musi mieć możliwość nadpisywania kategorii oraz tworzenia wyjątków – białe/czarne listy dla adresów URL.
5) Administrator musi mieć możliwość definiowania komunikatów zwracanych użytkownikowi dla różnych akcji podejmowanych przez moduł filtrowania.

Uwierzytelnianie użytkowników w ramach sesji

1) System Firewall musi umożliwiać weryfikację tożsamości użytkowników za pomocą:
   - Haseł statycznych i definicji użytkowników przechowywanych w lokalnej bazie systemu.
   - Haseł statycznych i definicji użytkowników przechowywanych w bazach zgodnych z LDAP.
   - Haseł dynamicznych (RADIUS, RSA SecurID) w oparciu o zewnętrzne bazy danych.
2) Musi istnieć możliwość zastosowania w tym procesie uwierzytelniania dwu-składnikowego.
3) Rozwiązanie powinno umożliwiać budowę architektury uwierzytelniania typu Single Sign On przy integracji ze środowiskiem Active Directory oraz zastosowanie innych mechanizmów: RADIUS lub API.

Zarządzanie

1) Elementy systemu bezpieczeństwa muszą mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH, jak i powinny mieć możliwość współpracy z dedykowanymi platformami centralnego zarządzania i monitorowania.
2) Komunikacja systemów zabezpieczeń z platformami centralnego zarządzania musi być realizowana z wykorzystaniem szyfrowanych protokołów.

3) Powinna istnieć możliwość włączenia mechanizmów uwierzytelniania dwu-składnikowego dla dostępu administracyjnego.
4) System musi współpracować z rozwiązaniami monitorowania poprzez protokoły SNMP w wersjach 2c, 3 oraz umożliwiać przekazywanie statystyk ruchu za pomocą protokołów netflow lub sflow.
5) System musi mieć możliwość zarządzania przez systemy firm trzecich poprzez API, do którego producent udostępnia dokumentację.
6) Element systemu pełniący funkcję Firewal musi posiadać wbudowane narzędzia diagnostyczne, przynajmniej: ping, traceroute, podglądu pakietów, monitorowanie procesowania sesji oraz stanu sesji firewall.

Logowanie

1) Elementy systemu bezpieczeństwa muszą realizować logowanie do aplikacji (logowania i raportowania) udostępnianej w chmurze, lub w ramach postępowania musi zostać dostarczony komercyjny system logowania i raportowania w postaci odpowiednio zabezpieczonej, komercyjnej platformy sprzętowej lub programowej.
2) W ramach logowania system pełniący funkcję Firewall musi zapewniać przekazywanie danych o zaakceptowanym ruchu, ruchu blokowanym, aktywności administratorów, zużyciu zasobów oraz stanie pracy systemu. Musi być zapewniona możliwość jednoczesnego wysyłania logów do wielu serwerów logowania.
3) Logowanie musi obejmować zdarzenia dotyczące wszystkich modułów sieciowych i bezpieczeństwa oferowanego systemu.
4) Musi istnieć możliwość logowania do serwera SYSLOG.

Certyfikaty

Poszczególne elementy oferowanego systemu bezpieczeństwa powinny posiadać następujące certyfikacje:

- ICSA lub EAL4 dla funkcji Firewall.
- ICSA dla funkcji IPS lub NSS Labs w kategorii NGFW.
- ICSA dla funkcji SSL VPN.

Serwisy i licencje

W ramach postępowania powinny zostać dostarczone licencje upoważniające do korzystania z aktualnych baz funkcji ochronnych producenta i serwisów. Powinny one obejmować:

Kontrola Aplikacji, IPS, Antywirus (z uwzględnieniem sygnatur do ochrony urządzeń mobilnych - co najmniej dla systemu operacyjnego Android), Analiza typu Sandbox, Antyspam, Web Filtering, bazy reputacyjne adresów IP/domen na okres 12 miesięcy.

Gwarancja oraz wsparcie

Gwarancja: System musi być objęty serwisem gwarancyjnym producenta przez okres 12 miesięcy, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości. W ramach tego serwisu producent musi zapewnić również dostęp do aktualizacji oprogramowania oraz wsparcie techniczne w trybie 8x5.

IV Szczegóły zamówienia

1. Serwis urządzeń

1.1. Zamawiający wymaga objęcia urządzeń serwisem od momentu rozpoczęcia obsługi konserwacyjno-serwisowej tj. od dnia podpisania umowy. Obsługa konserwacyjno-serwisowa obejmuje:

1.1.1. niezbędne do prawidłowego i ciągłego funkcjonowania: przeglądy, czyszczenie z zewnątrz i wewnątrz, regulacje, naprawy, wymianę uszkodzonych części i podzespołów,

1.1.2. wykonanie przeglądu i konserwacji każdego urządzenia z częstotliwością zgodną z zaleceniami producenta, jednak nie rzadziej, niż raz na pół roku, niezależnie od ilości wykonanych przez to urządzenie kopii/wydruków. Wykonanie każdego przeglądu zostanie potwierdzone wpisem w książce serwisowej, prowadzonej oddzielnie dla każdego urządzenia. Podstawowy zakres czynności wykonywanych podczas przeglądu:

1.1.2.1. Kontrola i czyszczenie urządzenia wewnątrz,

1.1.2.2. Kontrola, czyszczenie i regulacja układu optycznego (jeśli jest),

1.1.2.3. Kontrola i regulacja rolek pobierających i transportujących papier,

1.1.2.4. Kontrola, czyszczenie i regulacja zespołu nanoszenia,

1.1.2.5. Kontrola, czyszczenie i regulacja zespołu utrwalania,

1.1.2.6. Kontrola, czyszczenie i regulacja sekcji skanera (jeśli jest),

1.1.2.7. Diagnostyka ogólna urządzenia,

1.1.2.8. W przypadku urządzeń kolorowych przeprowadzenie kontroli stabilności kolorów, kontroli i kalibracji kolorów, kontroli oprogramowania odpowiedzialnego za stabilizację i kalibrację kolorów

1.1.2.9. Czyszczenie i kosmetyka obudowy urządzenia,

wykonanie kopii kontrolnej,

1.1.3. Okresowe sprawdzanie jakości kopii z wykorzystaniem karty testowej producenta danego urządzenia. Zamawiającemu przysługuje prawo do weryfikacji jakości kopii i reklamacji ich jakości. Reklamacja taka traktowana będzie jako zgłoszenie awarii,

1.1.4. Dostawę tonerów oraz innych materiałów eksploatacyjnych (poza papierem) w ilości wynikającej z rzeczywistego miesięcznego nakładu kopii/wydruków. Dostawa będzie następować na podstawie zgłoszeń Zamawiającego w ciągu **8 godzin roboczych Zamawiającego** od przekazania zgłoszenia przy użyciu środków komunikacji elektronicznej lub telefonicznie. Każda ze stron niezwłocznie potwierdza fakt ich otrzymania. W przypadku braku niezwłocznego potwierdzenia otrzymania wiadomości przez wykonawcę, Zamawiający przyjmuje, że pismo przekazane przez

Zamawiającego na adres e-mail podany przez wykonawcę zostało doręczone w sposób umożliwiający zapoznanie i będzie traktowany jako potwierdzenie otrzymania dokumentu przez wykonawcę.

1.1.5. W przypadku drukarek niebędących własnością Zamawiającego, zainstalowanych i pracujących w Wydziale Komunikacji i Transportu w systemie POJAZD/KIEROWCA, zgodnie z zapisami umowy pomiędzy PowiatemWłoszczowskim, a Polską Wytwórnią Papierów Wartościowych Zamawiający wymaga dostawy oryginalnych materiałów eksploatacyjnych. Urządzenia te pracują w odseparowanej galwanicznie sieci komputerowej i nie będą podlegać automatycznemu monitoringowi zużycia materiałów, w związku z tym, za monitorowanie zużycia materiałów odpowiadać będą służby informatyczne Zamawiającego. Ze względu na specyfikę pracy Wydziału Komunikacji i Transportu, Zamawiający wymaga, aby Wykonawca dostarczał Zamawiającemu materiały eksploatacyjne z wyprzedzeniem, tj. w taki sposób, aby Zamawiający posiadał ciągle przynajmniej 2 tonery do drukarek w zapasie. Zapewni to ciągłość pracy wszystkich punktów obsługi interesanta. Wszelkie naprawy pracujących w systemie drukarek realizowane są przez CEPIK, stąd Wykonawca ogranicza się w ich przypadku jedynie do dostawy materiałów eksploatacyjnych.

1.1.6. Zamawiający jednocześnie, zastrzega, że w przypadku zmiany urządzeń, o których mowa w punkcie 1.1.5 wykonawca winien dostarczyć materiały eksploatacyjne zgodnych ze wskazanymi urządzeniami.

1.1.7. Wykonawca odpowiada za odbiór zużytych pojemników po materiałach eksploatacyjnych i zużytych części zamiennych bezpośrednio po zainstalowaniu nowych oraz dokonywanie ich utylizacji zgodnie z obowiązującymi przepisami.

1.2. Obsługa konserwacyjno-serwisowa urządzeń wykonywana będzie w godzinach pracy Zamawiającego, jeżeli przerwa w korzystaniu z danego urządzenia nie będzie dłuższa niż 2 godziny.

1.3. Wykonawca jest zobowiązany do informowania Zamawiającego o uszkodzeniach i awariach urządzeń, których przyczyną może być zła jakość papieru, jednakże awarie takie i uszkodzenia wchodzą w zakres obsługi konserwacyjno-serwisowej i nie będą podstawą do roszczeń finansowych.

2. Obsługa awarii

2.1. Wykonawca zobowiązany jest do usunięcia awarii urządzeń **w ciągu 16 godzin roboczych Zamawiającego** od otrzymania zgłoszenia; zgłoszenie awarii odbywać się będzie przy użyciu środków komunikacji elektronicznej lub telefonicznie. W przypadku braku niezwłocznego potwierdzenia otrzymania wiadomości elektronicznej przez wykonawcę, Zamawiający przyjmuje, że pismo przekazane przez Zamawiającego na adres e-mail podany przez wykonawcę

zostało doręczone w sposób umożliwiający zapoznanie i będzie traktowany jako potwierdzenie otrzymania dokumentu przez wykonawcę.

2.2. W przypadku braku możliwości usunięcia awarii urządzenia w czasie określonym powyżej Wykonawca dostarczy na czas naprawy urządzenie zastępcze o parametrach nie gorszych niż urządzenie, które uległo awarii. Urządzenie zastępcze zostanie zainstalowane i skonfigurowane identycznie jak urządzenie, które uległo awarii, w takim terminie, by łączny przestój urządzenia **nie przekroczył 16 godzin roboczych Zamawiającego**,

2.3. Zamawiający wymaga, aby Wykonawca wymienił urządzenie, które uległo kolejno po sobie 3 takim samym awariom lub które uległo kolejno po sobie 5 jakichkolwiek awariom w okresie trzech miesięcy, na urządzenie nowe o takich samych parametrach lub lepszych oraz dokonał konfiguracji nowego urządzenia zgodnie z dotychczasową konfiguracją.

2.4. W przypadku wystąpienia nieprawidłowości w pracy systemu zarządzania wydrukami spowodowanych sterownikami dostarczonymi przez Wykonawcę, jest on zobowiązany do usunięcia nieprawidłowości w pracy sterowników **w terminie 7 dni**.

2.5. W przypadku awarii jednego z elementów systemów, Zamawiający wymaga, aby czas reakcji ze strony Wykonawcy wynosił 4 godziny robocze (przy dostępie zdalnym do systemu).

2.6. W przypadku nie wywiązania się Wykonawcy z obowiązków opisanych powyżej, Zamawiający zastrzega sobie prawo do naprawy, usunięcia awarii lub nieprawidłowości na koszt Wykonawcy.

3. Instalacja i uruchomienie urządzeń

3.1. Zamawiający zapewni swobodnie dostępne miejsce ustawienia urządzeń, z pojedynczym przyłączem energetycznym (230 V, 50 Hz) oraz pojedynczym przyłączem sieci Ethernet (RJ-45) i przydzieli po jednym adresie IP na urządzenie. Urządzenia będące własnością Zamawiającego zostaną objęte opieką serwisową zgodnie z dotychczasowym, przyjętym modelem instalacyjnym.

3.2. Instalacja i uruchomienie (wdrożenie) urządzeń obejmuje:

3.2.1. uruchomienie urządzeń w lokalizacjach wskazanych przez Zamawiającego, w tym:

3.2.1.1. podłączenie urządzeń do sieci elektrycznej i logicznej;

3.2.1.2. instalację wszystkich materiałów eksploatacyjnych (z wyjątkiem papieru) niezbędnych do prawidłowej pracy urządzeń,

3.2.1.3. zaprogramowanie poszczególnych funkcji urządzeń zgodnie ze specyfikacją,

3.2.1.4. konfiguracjęurządzeń z oprogramowaniem zarządzająco-monitorującym

3.2.1.5. przeszkolenie wskazanych przez Zamawiającego osób, w szczególności w zakresie obsługi urządzeń, którą zgodnie

z instrukcją obsługi Zamawiający może wykonywać samodzielnie, w tym usuwanie zacięć papieru, uzupełnianie kaset na papier itp.

3.2.1.6. przekazanie Zamawiającemu w formie papierowej i elektronicznej dokumentacji powdrożeniowej, sporządzonej w języku polskim, zawierającej:

- wykaz urządzeń na dzień zakończenia wdrożenia z podaniem lokalizacji, numerów seryjnych urządzeń i stanów początkowych liczników;
- instrukcje obsługi urządzeń.

4. **Dostawca winien mieć wiedzę i doświadczenie w zakresie instalacji i obsługi serwisowej oferowanych urządzeń.**

V. **Okres obowiązywania umowy:** od 02.01.2020 r. do 31.12.2020 r.

VI. **Termin wdrożenia:** do 31.12.2019r. Urządzenia zostaną dostarczone na ryzyko i koszt Wykonawcy do siedziby Zamawiającego. Po zakończeniu trwania umowy urządzenia o których mowa § 1 ust. 2 pkt 1 i 2 zostaną na ryzyko i koszt Wykonawcy odebrane, natomiast urządzenie, o którym mowa § 1 ust. 2 pkt 3 przechodzi na własność zamawiającego.

VII. **Dzierżawa zamawianych urządzeń** obejmuje czynsz dzierżawny oraz opłatę za faktyczną liczbę wykonanych kopii na poszczególnych urządzeniach.

VIII. **Zamawiający dokona oceny ważnych ofert na podstawie kryterium**:

CENA – 100%.

Na potrzeby wyłonienia najkorzystniejszej oferty zamawiający przyjął kryteria:
A1 – roczny abonament za dzierżawę urządzeń wielofunkcyjnych
A2 – roczny abonament za dzierżawę drukarek monochropmatycznych
A2 – roczny abonament za dzierżawę UTMa
B1 – cena za stronę wydruku A4 na urządzeniu wielofunkcyjnym mono x 100.000 kopii
B2 – cena za stronę wydruku A3 na urządzeniu wielofunkcyjnym mono x 100.000 kopii
B3 – cena za stronę wydruku A4 na urządzeniu wielofunkcyjnym kolor x 100.000 kopii
B4 – cena za stronę wydruku A3 na urządzeniu wielofunkcyjnym kolor x 100.000 kopii
B5 – cena za stronę wydruku A4 na drukarce monochromatycznej x 100.000 kopii
B6 –cena toner dla drukarek monochromatycznych OKI x 30 sztuk

A1+A2+B1+B2+B3+B4+B5+B6

IX. **Miejsce i termin złożenia oferty.** Oferty należy składać w siedzibie zamawiającego tj. Biurze Podawczym Starostwa Powiatowego we Włoszczowie ul. Wiśniowa 10, 29-100 Włoszczowa do dnia 11.12.2019r. do godziny 15:00. Decyduje data wpływu oferty do Starostwa. Oferty złożone po w/w terminie nie będą rozpatrywane.

Ofertę należy sporządzić w formie pisemnej zgodnie z załącznikiem. Ofertę należy złożyć w nieprzejrzystym i zamkniętym opakowaniu uniemożliwiającym otwarcie i zapoznania się z jej treścią przed upływem terminu otwarcia. Opakowania winny być zaadresowane na adres zamawiającego z dopiskiem "**Kompleksowa obsługa serwisowa wraz z**

dzierżawą urządzeń drukujących, kopiujących, dostawę materiałów eksploatacyjnych i zabezpieczeniem sieci"

X. **Warunki płatności**. Zamawiający będzie dokonywał miesięcznych płatności abonamentu oraz ponosił koszty wydruku stanowiący iloczyn miesięcznie wydrukowanych stron oraz kosztu jednostkowego ich wydruku, w terminie 14 dni od dnia otrzymania faktury na wskazany w niej rachunek bankowy.

XI. **Osoba do kontaktu:**
- Mariusz Wiśniewski – Kierownik Wydziału Administracyjno – Gospodarczego tel. 41 39 44 977 – zagadnienia merytoryczne
- Rafał Żmuda – Informatyk tel. 690 137 467 – zagadnienia techniczne

STAROSTA WŁOSZCZOWSKI
Dariusz Czechowski