|  |  |
| --- | --- |
| Numer sprawy: IRL.271.11.2024 | Stoczek Łukowski dnia 12.11.2024r |
| Miasto Stoczek Łukowski  Plac Tadeusza Kościuszki 1  21-450 Stoczek Łukowski  SZCZEGÓŁOWY OPIS PRZEDMIOTU ZAMÓWIENIA  pn. ROZWÓJ CYBERBEZPIECZEŃSTWA ORAZ UZUPEŁNIENIE INFRASTRUKTURY SPRZĘTOWEJ  DLA PROJEKTU  ROZWÓJ E-USŁUG I INFORMATYZACJA OPOLA LUBELSKIEGO ORAZ GMIN PARTNERSKICH DROGĄ DO TRANSFORMACJI CYFROWEJ  DOTYCZĄCY MIASTA STOCZEK ŁUKOWSKI | |

Spis treści

[1. Zestawienie ilościowe. 3](#_Toc180346880)

[2. Wymagania ogólne w zakresie dostawy sprzętu i oprogramowania. 3](#_Toc180346881)

[3. Proces współpracy. 5](#_Toc180346882)

[4. Zasada równoważności rozwiązań i neutralności technologicznej. 6](#_Toc180346883)

[5. Szczegółowy opis przedmiotu zamówienia. 8](#_Toc180346884)

[5.1. Wyposażenie serwerowni - zakup serwera z systemem operacyjnym (1 szt.). 8](#_Toc180346885)

[5.2. Wyposażenie serwerowni - zakup licencji oprogramowania antywirusowego (1 szt.). 11](#_Toc180346886)

[5.3. Wyposażenie stanowisk pracowniczych - zakup stacji roboczych (8 szt.). 18](#_Toc180346887)

[5.4. Wyposażenie stanowisk pracowniczych - zakup urządzenia wielofunkcyjnego (1 szt.). 22](#_Toc180346888)

# Zestawienie ilościowe.

|  |  |  |
| --- | --- | --- |
| Lp. | Nazwa | Ilość |
| 1. | Wyposażenie serwerowni - zakup serwera z systemem operacyjnym | 1 szt. |
| 2. | Wyposażenie serwerowni - zakup licencji oprogramowania antywirusowego | 1 szt. |
| 3. | Wyposażenie stanowisk pracowniczych - zakup stacji roboczych | 8 szt. |
| 4. | Wyposażenie stanowisk pracowniczych - zakup urządzenia wielofunkcyjnego | 1 szt. |

# Wymagania ogólne w zakresie dostawy sprzętu i oprogramowania.

1. Dostarczony sprzęt i oprogramowanie muszą być wolne od wad prawnych i fizycznych oraz nienoszący oznak użytkowania.
2. Dostarczony sprzęt i oprogramowanie muszą być fabrycznie nowe (tzn. wyprodukowane nie wcześniej, niż na 9 miesięcy przed ich dostarczeniem), muszą pochodzić z oficjalnego kanału sprzedaży producenta na rynek polski, pochodzić z seryjnej produkcji z uwzględnieniem opcji konfiguracyjnych przewidzianych przez producenta dla oferowanego modelu sprzętu i oprogramowania.
3. Niedopuszczalne są produkty prototypowe, nie dopuszcza się urządzeń długotrwale magazynowanych oraz pochodzących z programów wyprzedażowych producenta. Urządzenia nie mogą znajdować się na liście „end-of-sale”, „end-of-support”, „end-of-life” producenta.
4. Wymagana ilość i rozmieszczenie (na zewnątrz obudowy) jakichkolwiek portów nie może być osiągnięta w wyniku stosowania konwerterów, przejściówek, itp., niedopuszczalne jest zastosowanie jakichkolwiek zewnętrznych przejściówek czy konwerterów.
5. Wszystkie urządzenia będą zasilane bezpośrednio z sieci 230V.
6. Wykonawca zapewni dostawę do każdej wskazanej przez Zamawiającego lokalizacji.
7. Wykonawca jest odpowiedzialny za skonfigurowanie połączeń fizycznych, logicznych, podłączenie i skonfigurowanie urządzeń do działania, pozwalające na rozpoczęcie pracy oraz dostarczenie odpowiedniej ilości kabli zasilających, połączeniowych w celu przygotowania zamawianego sprzętu do działania.
8. Wykonawca zobowiązany jest do skonfigurowania zamawianego sprzętu w uzgodnieniu z Zamawiającym.
9. Prace instalacyjne będzie można realizować wyłącznie w terminach uzgodnionych z Zamawiającym.
10. Przedmiotem zamówienia jest wdrożenie nowego serwera do istniejącej infrastruktury oraz migracja danych do nowego serwera, w związku z tym Wykonawca musi przeprowadzić cały proces zgodnie z określonymi wymaganiami i dobrymi praktykami branżowymi, aby zapewnić bezpieczne, efektywne oraz bezawaryjne wdrożenie. Wykonawca musi przeprowadzić szczegółową analizę, która obejmie identyfikację istniejących serwerów, systemów operacyjnych, zasobów sieciowych oraz aplikacji, które obecnie działają w infrastrukturze. Wykonawca jest zobowiązany do oceny, jakie są wymagania dla nowego serwera, w tym rola, jaką ma pełnić, i zasoby sprzętowe, jakie będą potrzebne. Na tym etapie należy również zdefiniować wykorzystanie możliwości systemu operacyjnego oraz konfiguracji sprzętowej zaoferowanego serwera, uwzględniając redundancję (np. RAID dla dysków) oraz ewentualną możliwość przyszłej rozbudowy zasobów. Wykonawca jest zobowiązany do fizycznego montażu i uruchomienia serwera. Serwer powinien zostać odpowiednio skonfigurowany w szafie serwerowej, podłączony do sieci lokalnej (LAN) oraz zasilania. Po uruchomieniu serwera, należy skonfigurować jego interfejsy sieciowe, aby zapewnić jego widoczność w sieci. Następnie konieczna będzie instalacja wybranego systemu operacyjnego oraz podstawowych usług sieciowych. Wykonawca musi także zainstalować niezbędne aplikacje i usługi, które będą działały na nowym serwerze, zgodnie z ustaleniami z Zamawiającym, takimi jak serwery plików, aplikacji czy baz danych. Ponadto wykonawca musi skonfigurować wszystkie niezbędne protokoły sieciowe, takie jak SMB lub NFS, dla udostępniania zasobów. Dodatkowo Wykonawca w porozumieniu z Zamawiającym jest zobowiązany do przeprowadzenia migracji danych na nowy serwer w zakresie uzgodnionym z Zamawiającym. Wykonawca powinien przygotować dane do migracji, co obejmuje wykonanie pełnej kopii zapasowej wszystkich danych z istniejących serwerów i urządzeń NAS. W przypadku migracji baz danych migrację należy przeprowadzić przy użyciu narzędzi natywnych dla danej bazy (np. mysqldump dla MySQL). Wykonawca jest zobowiązany przeprowadzić migrację w sposób bezpieczny, zapewniając integralność i spójność danych. Po zakończeniu migracji, Wykonawca jest zobowiązany do przeprowadzenia weryfikacji poprawności danych, aby upewnić się, że wszystkie przeniesione pliki, bazy danych i aplikacje działają poprawnie w nowym środowisku. Wykonawca musi odpowiednio skonfigurować serwer w sieci, aby inne urządzenia miały do niego dostęp, oraz zapewnić, że użytkownicy mogą korzystać z nowych zasobów zgodnie z przydzielonymi im uprawnieniami. Dodatkowo, wszelkie usługi, takie jak serwery DNS, DHCP czy aplikacje, które działają na nowym serwerze, muszą zostać prawidłowo skonfigurowane i uruchomione. Po wdrożeniu serwera Wykonawca zobowiązany jest do przeprowadzenia testów w celu weryfikacji, że serwer działa zgodnie z oczekiwaniami Zamawiającego. Testy te powinny obejmować zarówno sprawdzenie dostępu do usług, jak i wydajności aplikacji oraz poprawności działania przeniesionych danych. Konieczne będzie również monitorowanie wydajności serwera oraz dostosowanie jego parametrów (np. alokacji zasobów CPU czy RAM), aby zoptymalizować jego działanie. Wykonawca jest zobowiązany również monitorować serwer przez 4 dni po wdrożeniu, aby upewnić się, że działa stabilnie i bez awarii. Wykonawca musi zagwarantować, że wdrożenie nowego serwera i migracja danych będą przeprowadzone w sposób bezpieczny, efektywny oraz zgodny z najlepszymi praktykami branżowymi, minimalizując ryzyko przestojów i zapewniając pełną funkcjonalność nowego serwera w istniejącej infrastrukturze.
11. Wykonawca będzie zobowiązany do złożenia dokumentacji powykonawczej, zawierającej w szczególności wszystkie dane dostępu do urządzeń i oprogramowania, które będą wykorzystywane podczas instalacji i konfiguracji sprzętu i oprogramowania.
12. Dla dostaw sprzętu informatycznego z oprogramowaniem Zamawiający wymaga fabrycznie nowego oprogramowania (nieużywanego nigdy wcześniej), w wersji z certyfikatem autentyczności dla każdej licencji, o ile producent oferowanego oprogramowania stosuje certyfikaty autentyczności. Wykonawca zobowiązany jest do dostarczenia fabrycznie nowego oprogramowania (w tym systemu operacyjnego) nieużywanego oraz nigdy wcześniej nieaktywowanego na innym urządzeniu oraz pochodzącego z legalnego źródła sprzedaży. W przypadku oprogramowania naklejka hologramowa winna być zabezpieczona przed możliwością odczytania klucza za pomocą zabezpieczeń stosowanych przez producenta, o ile producent oferowanego oprogramowania stosuje takie zabezpieczenia. Zamawiający zastrzega możliwość weryfikacji dostarczonego oprogramowania na etapie oceny ofert jak i na etapie dostawy pod kątem legalności oprogramowania bezpośrednio u producenta oprogramowania. Zamawiający zastrzega możliwość żądania od Wykonawcy na etapie dostawy przedstawienia dokumentów dotyczących zakupu oprogramowania (faktury, rachunki) w autoryzowanym kanale dystrybucyjnym producenta oprogramowania.

# Proces współpracy.

1. Wykonawca przygotuje projekt techniczny realizacji koncepcji, uwzględniający dobre praktyki i rekomendacje eksploatacyjne, po wykonaniu analizy istniejącego u Zamawiającego rozwiązania wraz z koncepcją uruchomienia sprzętu i oprogramowania oraz uwarunkowania organizacyjne i sprzętowe, łącznie zwane dalej projektem technicznym. W projekcie technicznym muszą być zawarte:
2. opis koncepcji realizacji prac przy wykorzystaniu dostarczonego oprogramowania i sprzętu,
3. scenariusze testowe, procedury oraz wzory raportów testów,
4. szczegółowy harmonogram realizacji prac wdrożeniowych i migracyjnych, uwzględniający specyfikę organizacji Zamawiającego,
5. zalecenia przedwdrożeniowe dla Zamawiającego, jeżeli będą wymagane.
6. Akceptacja projektu technicznego wraz z procedurami oraz wzorami raportów z testów będzie podlegała następującej procedurze:
7. Wykonawca przekaże do akceptacji Zamawiającego, drogą elektroniczną projekt techniczny wraz z procedurami oraz wzorami raportów z testów, w terminie nie dłuższym niż 30 dni kalendarzowych od dnia zawarcia umowy,
8. Zamawiający w terminie nie dłuższym niż 7 dni roboczych od dnia dostarczenia przez Wykonawcę kompletnych dokumentów, poinformuje Wykonawcę o ich akceptacji lub konieczności wprowadzenia zmian,
9. wszystkie uwagi do dokumentów zgłoszone przez Zamawiającego zostaną wprowadzone przez Wykonawcę, w terminie nie dłuższym niż 5 dni roboczych od dnia ich otrzymania,
10. Zamawiający w terminie 5 dni roboczych od dnia powtórnego dostarczenia przez Wykonawcę poprawionych dokumentów, poinformuje Wykonawcę o ich akceptacji lub konieczności wprowadzenia zmian,
11. w przypadku nieuwzględnienia uwag Zamawiającego, Zamawiający zastrzega sobie prawo do wskazania ostatecznego terminu dostarczenia projektu technicznego wraz z procedurami oraz wzorami raportów z testów,
12. zatwierdzony projekt techniczny wraz procedurami zostaną przekazane Zamawiającemu w 1 egzemplarzu oraz w formie elektronicznej na pendrive, w postaci plików do edycji i PDF.
13. Wykonawca zrealizuje wdrożenie produkcyjne sprzętu zgodnie z zakresem prac i projektem technicznym.
14. Wykonawca przeprowadzi testy akceptacyjne wdrożonych rozwiązań. Wykonawca opracuje koncepcję backupu dla wdrożonej infrastruktury opierając się na będącym częścią infrastruktury sprzętowo-systemowej Zamawiającego systemie backup.
15. Wykonawca opracuje i przedstawi raport z testów. W przypadku zrealizowania scenariusza testowego z wynikiem negatywnym, Wykonawca przedstawi nowe rozwiązanie wadliwego elementu systemu i przeprowadzi ponowny test wg scenariusza, w terminie wyznaczonym przez Zamawiającego, dochowując terminu wykonania Umowy. Raport z testów powinien zawierać listę przeprowadzonych testów wraz z ich wynikiem.
16. Wykonawca opracuje dokumentację powykonawczą oraz procedury administracyjne i eksploatacyjne w zakresie uzgodnionym z Zamawiającym, w tym: dokumentację wdrożeniową, procedury operacyjne, procedury „Disaster Recovery”. Akceptacja dokumentacji powykonawczej będzie przebiegała zgodnie z zasadami określonymi dla akceptacji projektu technicznego.

Instruktaże.

1. Instruktaże stanowiskowe będą prowadzone w języku polskim w siedzibie Zamawiającego i obejmą zakresem m.in.: użytkowane oprogramowanie; budowę, architekturę i konfigurację rozwiązania; administrowanie wdrożonym rozwiązaniem.
2. Instruktaże stanowiskowe zostaną przeprowadzone przez osoby prowadzące prace wdrożeniowe w ramach niniejszego zamówienia.
3. Instruktaże powinny trwać minimum 16 godzin lekcyjnych (45 minut) i będą przeprowadzone dla wskazanej przez Zamawiającego liczby osób (maksymalnie 4 osoby).
4. Zamawiający nie dopuszcza przeprowadzenia instruktaży w trybie zdalnym (online).
5. Administratorzy rozwiązania po zakończeniu Instruktaży stanowiskowych muszą w szczególności umieć wykonywać czynności administracyjne związane z obsługą, utrzymaniem i monitoringiem sprzętu, znać i umieć realizować procedury backupu. Ponadto powinni znać typowe zagrożenia i problemy związane z funkcjonowaniem rozwiązania, a także sposoby ich przeciwdziałania, wykrywania i usuwania. Powinni umieć instalować, konfigurować, rekonfigurować, monitorować i prawidłowo eksploatować wdrożone rozwiązanie, jak również znać jego wdrożoną konfigurację.

# Zasada równoważności rozwiązań i neutralności technologicznej.

1. Za równoważne do wyspecyfikowanego rozwiązania Zamawiający uzna rozwiązanie o tym samym przeznaczeniu, cechach technicznych, jakościowych i funkcjonalnych odpowiadających cechom technicznym, jakościowym i funkcjonalnym wskazanych w opisie przedmiotu zamówienia, lub lepszych, oznaczonych innym znakiem towarowym, patentem lub pochodzeniem.
2. Rozwiązanie równoważne musi pozwalać na zrealizowanie zakładanego przez Zamawiającego celu poprzez parametry wydajnościowe i funkcjonalne, mające wpływ na skuteczność działania, takie same lub lepsze od wskazanych wymagań minimalnych.
3. Użycie w opisie przedmiotu zamówienia nazw rozwiązań służy ustaleniu minimalnego standardu wykonania i określenia właściwości i wymogów technicznych założonych w dokumentacji technicznej dla projektowanych rozwiązań lub też stosowane jest w celu wskazania aktualnie użytkowanego środowiska Zamawiającego, z którym rozwiązanie równoważne powinno być kompatybilne.
4. Wykonawca zobligowany jest do wykazania, że oferowane rozwiązania równoważne spełnią zakładane wymagania minimalne. Wykonawca, który złoży ofertę na produkty równoważne musi do oferty załączyć dokumenty zawierające dokładny opis oferowanych produktów, z którego wynikać będzie zachowanie warunków równoważności. Wykonawca, który posługuje się równoważnymi certyfikatami musi je załączyć do oferty. Przez certyfikat równoważny Zamawiający rozumie certyfikat analogiczny co do zakresu z certyfikatami wskazanymi z nazwy, który potwierdza spełnianie normy charakteryzującej się cechami właściwymi dla normy wymienionej przez Zamawiającego, wystawiony przez niezależny podmiot uprawniony do wystawiania certyfikatów.
5. Brak określenia „minimum” oznacza wymaganie na poziomie minimalnym, a Wykonawca może zaoferować rozwiązanie o lepszych parametrach.
6. W celu zachowania zasad neutralności technologicznej i konkurencyjności dopuszcza się rozwiązania równoważne do wyspecyfikowanych, przy czym za rozwiązanie równoważne uważa się takie rozwiązanie, które pod względem technologii, wydajności i funkcjonalności nie odbiega lub jest lepsze od technologii funkcjonalności i wydajności wyszczególnionych w rozwiązaniu wyspecyfikowanym.
7. Nie podlegają porównaniu cechy rozwiązania właściwe wyłącznie dla rozwiązania wyspecyfikowanego, takie jak: zastrzeżone patenty, własnościowe rozwiązania technologiczne, własnościowe protokoły itp., a jedynie te, które stanowią o istocie całości zakładanych rozwiązań technologicznych i posiadają odniesienie w rozwiązaniu równoważnym. W związku z tym, Wykonawca może zaproponować rozwiązania, które realizują takie same funkcjonalności wyspecyfikowane przez Zamawiającego w inny, niż podany sposób.
8. Przez bardzo zbliżoną (podobną) wartość użytkową rozumie się podobne, z dopuszczeniem nieznacznych różnic nie wpływających w żadnym stopniu na całokształt systemu, zachowanie oraz realizowanie podobnych funkcjonalności w danych warunkach, dla których to warunków rozwiązania te są dedykowane. Rozwiązanie równoważne musi zawierać dokumentację potwierdzającą, że spełnia wymagania funkcjonalne Zamawiającego, w tym wyniki porównań, testów czy możliwości oferowanych przez to rozwiązanie w odniesieniu do rozwiązania wyspecyfikowanego.
9. W przypadku wskazania przez Zamawiającego określonych testów wydajności Zamawiający zastrzega, iż w celu sprawdzenia poprawności przeprowadzonych testów może wezwać Wykonawcę do przedstawienia wskazanego przez Zamawiającego oprogramowania testującego wraz z testowanym urządzeniem i/lub oprogramowaniem. Wszystkie testy wydajnościowe wykonawca musi przeprowadzić w oferowanej konfiguracji, przy automatycznych ustawieniach konfiguratora oprogramowania testującego i natywnej rozdzielczości wyświetlacza oraz włączonych wszystkich urządzaniach. Nie dopuszcza się stosowania overclokingu, oprogramowania wspomagającego pochodzącego z innego źródła niż fabrycznie zainstalowane oprogramowanie przez producenta, ingerowania w ustawieniach BIOS (tzn. wyłączanie urządzeń stanowiących pełną konfigurację), jak również w samym środowisku systemu (tzn. zmniejszanie rozdzielczości, jasności i kontrastu itp.). Zamawiający dopuszcza prowadzenie testów wydajnościowych w oparciu o dowolny system operacyjny zainstalowany na urządzeniu.
10. W przypadku wskazania przez Zamawiającego określonych testów wydajności Zamawiający dopuszcza równoważne im testy wydajnościowe umożliwiające potwierdzenie zakładanych poziomów wydajności. W przypadku użycia przez Wykonawcę równoważnych testów wydajności Zamawiający zastrzega, iż w celu sprawdzenia równoważności przeprowadzonych testów Wykonawca może zostać wezwany do dostarczenia Zamawiającemu wskazanego przez Zamawiającego oprogramowania testującego i równoważnego do niego oprogramowania testującego wraz z testowanym urządzeniem i/lub oprogramowaniem. Wszystkie testy wydajnościowe wykonawca musi przeprowadzić w oferowanej konfiguracji, przy automatycznych ustawieniach konfiguratora oprogramowania testującego i natywnej rozdzielczości wyświetlacza oraz włączonych wszystkich urządzaniach. Nie dopuszcza się stosowania overclokingu, oprogramowania wspomagającego pochodzącego z innego źródła niż fabrycznie zainstalowane oprogramowanie przez producenta, ingerowania w ustawieniach BIOS (tzn. wyłączanie urządzeń stanowiących pełną konfigurację), jak również w samym środowisku systemu (tzn. zmniejszanie rozdzielczości, jasności i kontrastu itp.). Zamawiający dopuszcza prowadzenie testów wydajnościowych w oparciu o dowolny system operacyjny zainstalowany na urządzeniu.
11. Dodatkowo, wszędzie tam, gdzie zostało wskazane pochodzenie (marka, znak towarowy, producent, dostawca itp.) materiałów lub normy, aprobaty, specyfikacje i systemy, o których mowa w ustawie Prawo Zamówień Publicznych (zwana dalej ustawą), Zamawiający dopuszcza oferowanie sprzętu lub rozwiązań równoważnych pod warunkiem, że zapewnią uzyskanie parametrów technicznych takich samych lub lepszych niż wymagane przez Zamawiającego w dokumentacji przetargowej. Zamawiający dopuszcza oferowanie materiałów lub urządzeń równoważnych. Materiały lub urządzenia pochodzące od konkretnych producentów określają minimalne parametry jakościowe i cechy użytkowe, a także jakościowe (m.in.: wymiary, skład, zastosowany materiał, kolor, odcień, przeznaczenie materiałów i urządzeń, estetyka itp.) jakim muszą odpowiadać materiały lub urządzenia oferowane przez Wykonawcę, aby zostały spełnione wymagania stawiane przez Zamawiającego. Operowanie przykładowymi nazwami producenta ma jedynie na celu doprecyzowanie poziomu oczekiwań Zamawiającego w stosunku do określonego rozwiązania. Posługiwanie się nazwami producentów / produktów ma wyłącznie charakter przykładowy. Zamawiający, wskazując oznaczenie konkretnego producenta (dostawcy), konkretny produkt lub materiały przy opisie przedmiotu zamówienia, dopuszcza jednocześnie produkty równoważne o parametrach jakościowych i cechach użytkowych co najmniej na poziomie parametrów wskazanego produktu, uznając tym samym każdy produkt o wskazanych lub lepszych parametrach. Zamawiający opisując przedmiot zamówienia przy pomocy określonych norm, aprobat czy specyfikacji technicznych i systemów odniesienia dopuszcza rozwiązania równoważne opisywanym. Wykonawca, który powołuje się na rozwiązania równoważne opisywanym przez Zamawiającego, jest obowiązany wykazać, że oferowane przez niego dostawy spełniają wymagania określone przez Zamawiającego. W takiej sytuacji Zamawiający wymaga złożenia stosownych dokumentów uwiarygodniających te rozwiązania.

# Szczegółowy opis przedmiotu zamówienia.

# Wyposażenie serwerowni - zakup serwera z systemem operacyjnym (1 szt.).

Minimalne parametry techniczne serwera:

1. Obudowa typu RACK o wysokości maksymalnie 2U z możliwością instalacji do 12 dysków 3.5" Hot-Plug, z kompletem szyn umożliwiających montaż w szafie RACK i wysuwanie serwera do celów serwisowych oraz organizatorem do kabli.
2. Płyta główna z możliwością zainstalowania dwóch procesorów.
3. Zainstalowane dwa procesory ośmiordzeniowe klasy x86 dedykowane do pracy z oferowanym serwerem, umożliwiające osiągnięcie przez serwer wyniku co najmniej 250 punktów w teście SPECrate2017\_fp\_base dla konfiguracji dwuprocesorowej według wyników publikowanych na stronie [www.spec.org](http://www.spec.org). Zamawiający żąda załączenia do oferty przedmiotowego środka dowodowego określonego w SWZ potwierdzającego spełnienie dla procesora dedykowanego do pracy z zaoferowanym serwerem żądanej przez Zamawiającego wydajności.
4. Pamięć RAM: zainstalowane min. 256 GB, płyta główna musi obsługiwać do min. 1 TB pamięci RAM DDR5.
5. Zabezpieczenia pamięci RAM: Memory Rank Sparing i/lub Memory Mirror i/lub Single Device Data Correction i/lub Memory Lockstep i/lub Chipkill i/lub Extended ECC i/lub Advanced Memory Device Correction i/lub AMD Memory Guard i/lub ECC.
6. Co najmniej jeden wolny slot PCIe x8 generacji 4 w celu możliwości rozbudowy serwera.
7. Zintegrowana karta graficzna ze złączem VGA.
8. Interfejsy sieciowe: Wbudowane co najmniej 4 interfejsy sieciowe 10Gb Ethernet w standardzie 10GBaseT oraz 2 interfejsy sieciowe 25Gb Ethernet w standardzie SFP28.
9. Dyski twarde: Możliwość instalacji dysków SATA, SAS, SSD. Zainstalowane dyski: 3 dyski twarde Hot-Plug SSD SAS o prędkości min. 24 Gb/s o pojemności co najmniej 1,92 TB każdy oraz 5 dysków twardych Hot-Plug NL-SAS o prędkości min. 12 Gb/s o pojemności co najmniej 4 TB każdy. W przypadku uszkodzenia dysku w okresie gwarancji Zamawiający wymaga by uszkodzony dysk pozostał jego własnością.
10. Możliwość zainstalowania co najmniej dwóch dysków M.2 SATA z możliwością konfiguracji RAID 1.
11. Możliwość zainstalowania dedykowanego modułu dla hypervisora wirtualizacyjnego, wyposażonego w co najmniej dwa nośniki typu flash z możliwością konfiguracji zabezpieczenia synchronizacji pomiędzy nośnikami z poziomu BIOS serwera, rozwiązanie nie może powodować zmniejszenia ilości wnęk na dyski twarde.
12. Kontroler RAID: Sprzętowy kontroler dyskowy umożliwiający konfiguracje poziomów RAID: 0, 1, 5, 6, 10, 50, 60.
13. Wsparcie dla dysków samoszyfrujących.
14. Wbudowane porty: min. 3 porty USB, w tym co najmniej 2 porty USB 3.x, co najmniej 1 port USB musi być dostępny z przodu obudowy. Dodatkowo min. jeden port dedykowany dla karty zarządzającej dostępny z przodu obudowy. Ilość dostępnych portów USB nie może być osiągnięta poprzez stosowanie zewnętrznych przejściówek, rozgałęziaczy czy dodatkowych kart rozszerzeń zajmujących jakikolwiek slot PCI Express serwera.
15. Wentylatory: Redundantne typu Hot Plug.
16. Zasilacze: Redundantne typu Hot Plug o mocy nieprzekraczającej 1100 W każdy.
17. Karta zarządzania: Niezależna od zainstalowanego na serwerze systemu operacyjnego posiadająca dedykowane port RJ-45 Gigabit Ethernet umożliwiająca:
    1. zdalny dostęp do graficznego interfejsu Web karty zarządzającej,
    2. zdalne monitorowanie i informowanie o statusie serwera,
    3. szyfrowane połączenie oraz autentykacje i autoryzację użytkownika,
    4. możliwość podmontowania zdalnych wirtualnych napędów,
    5. wirtualną konsolę z dostępem do myszy, klawiatury,
    6. wsparcie dla IPv6,
    7. wsparcie dla SNMP; IPMI2.0, VLAN tagging, SSH,
    8. integracja z Active Directory,
    9. wsparcie dla dynamic DNS.
18. System bezpieczeństwa serwera realizowany poprzez następujące zabezpieczenia:
    1. wbudowane diody informacyjne lub wyświetlacz informujące o stanie serwera;
    2. blokada zamykana na klucz służąca do ochrony nieautoryzowanego dostępu do dysków twardych;
    3. moduł TPM 2.0;
    4. możliwość dynamicznego włączania i wyłączania portów USB na obudowie – bez potrzeby restartu serwera;
    5. możliwość wymazania danych ze znajdujących się dysków wewnątrz serwera – niezależne od zainstalowanego systemu operacyjnego, uruchamiane z poziomu zarządzania serwerem.
19. Wykonawca jest zobowiązany do dostawy wraz z serwerem systemu operacyjnego umożliwiającego zarządzenie serwerem klasy Microsoft Windows Serwer Standard w najnowszej wersji oferowanej przez producenta oprogramowania wraz z 15 licencjami dostępowymi umożliwiającymi korzystanie przez 15 użytkowników lub równoważnego systemu zgodnie z poniżej określonymi warunkami równoważności.

Warunki równoważności dla dostawy oprogramowania Microsoft Windows Serwer Standard w najnowszej wersji oferowanej przez producenta oprogramowania wraz z 15 licencjami dostępowymi Microsoft Windows Server 2022 CAL User:

* 1. Licencja musi uprawniać do uruchamiania serwerowego systemu operacyjnego w środowisku fizycznym i dwóch wirtualnych środowiskach serwerowego systemu operacyjnego za pomocą wbudowanych mechanizmów wirtualizacji oraz dostępu do serwerowego systemu operacyjnego dla minimum 15 użytkowników.
  2. Możliwość wykorzystywania 240 procesorów wirtualnych oraz 1TB pamięci RAM i dysku o pojemności min. 64TB przez każdy wirtualny serwerowy system operacyjny.
  3. Możliwość migracji maszyn wirtualnych bez zatrzymywania ich pracy między fizycznymi serwerami z uruchomionym mechanizmem wirtualizacji (hypervisor) przez sieć Ethernet, bez konieczności stosowania dodatkowych mechanizmów współdzielenia pamięci.
  4. Wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany pamięci RAM bez przerywania pracy.
  5. Wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany procesorów bez przerywania pracy.
  6. Automatyczna weryfikacja cyfrowych sygnatur sterowników w celu sprawdzenia czy sterownik przeszedł testy jakości przeprowadzone przez producenta systemu operacyjnego.
  7. Możliwość dynamicznego obniżania poboru energii przez rdzenie procesorów niewykorzystywane w bieżącej pracy.
  8. Mechanizm ten musi uwzględniać specyfikę procesorów wyposażonych w mechanizmy Hyper-Threading;
  9. Wbudowany mechanizm klasyfikowania i indeksowania plików (dokumentów) w oparciu o ich zawartość.
  10. Wbudowane szyfrowanie dysków przy pomocy mechanizmów posiadających certyfikat FIPS 140-2 lub równoważny wydany przez NIST lub inną agendę rządową zajmującą się bezpieczeństwem informacji.
  11. Możliwość uruchamianie aplikacji internetowych wykorzystujących technologię ASP.NET.
  12. Możliwość dystrybucji ruchu sieciowego HTTP pomiędzy kilka serwerów.
  13. Wbudowana zapora internetowa (firewall) z obsługą definiowanych reguł dla ochrony połączeń internetowych i intranetowych.
  14. Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, przeglądarka internetowa, pomoc, komunikaty systemowe.
  15. Możliwość zmiany języka interfejsu po zainstalowaniu systemu, dla co najmniej 2 języków poprzez wybór z listy dostępnych lokalizacji.
  16. Wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug&Play).
  17. Możliwość zdalnej konfiguracji, administrowania oraz aktualizowania systemu.
  18. Wsparcie dostępu do zasobu dyskowego SSO poprzez wiele ścieżek (Multipath).
  19. Możliwość instalacji poprawek poprzez wgranie ich do obrazu instalacyjnego.
  20. Mechanizmy zdalnej administracji oraz mechanizmy (również działające zdalnie) administracji przez skrypty.

1. Oferowany serwer musi znajdować się na liście Windows Server Catalog i posiadać status „Certified for Windows” dla systemów Microsoft Windows Server 2016, Microsoft Windows Server 2019, Microsoft Windows Server 2022.
2. Jakość produktu i sposobu jego wykonania: Certyfikat ISO 9001 lub inny równoważny dokument poświadczający, że producent serwera opracował, wdrożył i certyfikował system zarządzania jakością; Certyfikat ISO 50001 lub inny równoważny dokument poświadczający, że producent serwera posiada system zarządzania energią, zmniejszający zużycie energii, wpływy na środowisko i zwiększający rentowność; Deklaracja zgodności CE lub inny równoważny dokument poświadczający, ze oferowany serwer spełnia wszystkie zasadnicze wymagania zawarte w poszczególnych dyrektywach nowego podejścia przewidujących oznakowanie CE; Potwierdzenie spełnienia kryteriów środowiskowych, w tym zgodności z dyrektywą RoHS Unii Europejskiej o eliminacji substancji niebezpiecznych w postaci oświadczenia producenta serwera lub innego dokumentu potwierdzającego spełnienie kryteriów środowiskowych w tym zgodności z dyrektywą RoHS Unii Europejskiej o eliminacji substancji niebezpiecznych; Certyfikat NIST SP 800-193 lub inny równoważny dokument potwierdzający, że serwer spełnia wymagania normy NIST SP 800-193 ochrony przed cyberatakami. Zamawiający żąda załączenia do oferty przedmiotowych środków dowodowych - dokumentów potwierdzających spełnienie przez oferowany serwer i jego/ich producenta/producentów w zakresie określonym powyżej.
3. Gwarancja: min. 60 miesięcy gwarancji producenta obejmująca wszystkie komponenty serwera wchodzące w skład oferowanej konfiguracji realizowanej w miejscu instalacji sprzętu z czasem reakcji serwisu do następnego dnia roboczego od przyjęcia zgłoszenia, w przypadku awarii dyski Zamawiający wymaga, aby dyski pozostały u Zamawiającego. Możliwość zgłaszania awarii poprzez ogólnopolską linię telefoniczną producenta lub dedykowany portal techniczny producenta. W czasie obowiązywania gwarancji na sprzęt, możliwość weryfikacji - na podstawie numeru seryjnego urządzenia - pierwotnej konfiguracji sprzętowej serwera, w tym model i typ dysków twardych, procesora, ilość fabrycznie zainstalowanej pamięci operacyjnej, czasu obowiązywania i typ udzielonej gwarancji przez portal producenta serwera.

# Wyposażenie serwerowni - zakup licencji oprogramowania antywirusowego (1 szt.).

Aktualnie w urzędzie wykorzystywana jest oprogramowanie ESET Endpoint Antywirus ESET PROTECT Essential ON-PREM (ochrona stacji roboczych, urządzeń mobilnych, wirtualnych stacji mobilnych). Licencja udzielona jest do 2025-09-04, a obecna liczba stanowisk: 16. Dostarczone rozwiązanie powinno umożliwiać wykorzystanie istniejących licencji w celu optymalizacji kosztów. Dostarczone rozwiązanie musi łącznie z istniejącym oprogramowaniem musi mieć możliwość jednoczesnej pracy dla 20 użytkowników końcowych oraz umożliwić instalację na 15 stacjach roboczych oraz 3 serwerach w okresie 60 miesięcy oraz spełniać niżej określone minimalne wymogi funkcjonalne:

Administracja zdalna w chmurze.

1. Rozwiązanie musi być dostępne w chmurze producenta oprogramowania antywirusowego.
2. Rozwiązanie musi umożliwiać dostęp do konsoli centralnego zarządzania z poziomu interfejsu WWW.
3. Rozwiązanie musi być zabezpieczone za pośrednictwem protokołu SSL.
4. Rozwiązanie musi posiadać mechanizm wykrywający sklonowane maszyny na podstawie unikatowego identyfikatora sprzętowego stacji.
5. Rozwiązanie musi posiadać możliwość komunikacji agenta przy wykorzystaniu HTTP Proxy.
6. Rozwiązanie musi posiadać możliwość zarządzania urządzeniami mobilnymi – MDM.
7. Rozwiązanie musi posiadać możliwość wymuszenia dwufazowej autoryzacji podczas logowania do konsoli administracyjnej.
8. Rozwiązanie musi posiadać możliwość dodania zestawu uprawnień dla użytkowników w oparciu co najmniej o funkcje zarządzania: politykami, raportowaniem, zarządzaniem licencjami, zadaniami administracyjnymi. Każda z funkcji musi posiadać możliwość wyboru uprawnienia: odczyt, użyj, zapisz oraz brak.
9. Rozwiązanie musi posiadać minimum 80 szablonów raportów, przygotowanych przez producenta.
10. Rozwiązanie musi posiadać możliwość tworzenia grup statycznych i dynamicznych komputerów.
11. Grupy dynamiczne muszą być tworzone na podstawie szablonu określającego warunki, jakie musi spełnić klient, aby został umieszczony w danej grupie. Warunki muszą zawierać co najmniej: adresy sieciowe IP, aktywne zagrożenia, stan funkcjonowania/ochrony, wersja systemu operacyjnego, podzespoły komputera.
12. Rozwiązanie musi posiadać możliwość uruchomienia zadań automatycznie, przynajmniej z wyzwalaczem: wyrażenie CRON, codziennie, cotygodniowo, comiesięcznie, corocznie, po wystąpieniu nowego zdarzenia oraz umieszczeniu agenta w grupie dynamicznej.

Ochrona stacji roboczych.

1. Rozwiązanie musi wspierać systemy operacyjne Windows (Windows 10/Windows 11).
2. Rozwiązanie musi wspierać architekturę ARM64.
3. Rozwiązanie musi zapewniać wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor.
4. Rozwiązanie musi posiadać wbudowaną technologię do ochrony przed rootkitami oraz podłączeniem komputera do sieci botnet.
5. Rozwiązanie musi zapewniać wykrywanie potencjalnie niepożądanych, niebezpiecznych oraz podejrzanych aplikacji.
6. Rozwiązanie musi zapewniać skanowanie w czasie rzeczywistym otwieranych, zapisywanych i wykonywanych plików.
7. Rozwiązanie musi zapewniać skanowanie całego dysku, wybranych katalogów lub pojedynczych plików "na żądanie" lub według harmonogramu.
8. Rozwiązanie musi zapewniać skanowanie plików spakowanych i skompresowanych oraz dysków sieciowych i dysków przenośnych.
9. Rozwiązanie musi posiadać opcję umieszczenia na liście wykluczeń ze skanowania wybranych plików, katalogów lub plików na podstawie rozszerzenia, nazwy, sumy kontrolnej (SHA1) oraz lokalizacji pliku.
10. Rozwiązanie musi integrować się z Intel Threat Detection Technology.
11. Rozwiązanie musi zapewniać skanowanie i oczyszczanie poczty przychodzącej POP3 i IMAP „w locie” (w czasie rzeczywistym), zanim zostanie dostarczona do klienta pocztowego, zainstalowanego na stacji roboczej (niezależnie od konkretnego klienta pocztowego).
12. Rozwiązanie musi zapewniać skanowanie ruchu sieciowego wewnątrz szyfrowanych protokołów HTTPS, POP3S, IMAPS.
13. Rozwiązanie musi posiadać wbudowane dwa niezależne moduły heurystyczne – jeden wykorzystujący pasywne metody heurystyczne i drugi wykorzystujący aktywne metody heurystyczne oraz elementy sztucznej inteligencji. Musi istnieć możliwość wyboru, z jaką heurystyka ma odbywać się skanowanie – z użyciem jednej lub obu metod jednocześnie.
14. Rozwiązanie musi zapewniać blokowanie zewnętrznych nośników danych na stacji w tym przynajmniej: Pamięci masowych, optycznych pamięci masowych, pamięci masowych Firewire, urządzeń do tworzenia obrazów, drukarek USB, urządzeń Bluetooth, czytników kart inteligentnych, modemów, portów LPT/COM oraz urządzeń przenośnych.
15. Rozwiązanie musi posiadać funkcję blokowania nośników wymiennych bądź grup urządzeń ma umożliwiać użytkownikowi tworzenie reguł dla podłączanych urządzeń minimum w oparciu o typ, numer seryjny, dostawcę lub model urządzenia.
16. Moduł HIPS musi posiadać możliwość pracy w jednym z pięciu trybów:
    1. tryb automatyczny z regułami, gdzie program automatycznie tworzy i wykorzystuje reguły wraz z możliwością wykorzystania reguł utworzonych przez użytkownika,
    2. tryb interaktywny, w którym to rozwiązanie pyta użytkownika o akcję w przypadku wykrycia aktywności w systemie,
    3. tryb oparty na regułach, gdzie zastosowanie mają jedynie reguły utworzone przez użytkownika,
    4. tryb uczenia się, w którym rozwiązanie uczy się aktywności systemu i użytkownika oraz tworzy odpowiednie reguły w czasie określonym przez użytkownika. Po wygaśnięciu tego czasu program musi samoczynnie przełączyć się w tryb pracy oparty na regułach,
    5. tryb inteligentny, w którym rozwiązanie będzie powiadamiało wyłącznie o szczególnie podejrzanych zdarzeniach.
17. Rozwiązanie musi być wyposażone we wbudowaną funkcję, która wygeneruje pełny raport na temat stacji, na której zostało zainstalowane, w tym przynajmniej z: zainstalowanych aplikacji, usług systemowych, informacji o systemie operacyjnym i sprzęcie, aktywnych procesów i połączeń sieciowych, harmonogramu systemu operacyjnego, pliku hosts, sterowników.
18. Funkcja, generująca taki log, ma posiadać przynajmniej 9 poziomów filtrowania wyników pod kątem tego, które z nich są podejrzane dla rozwiązania i mogą stanowić zagrożenie bezpieczeństwa.
19. Rozwiązanie musi posiadać automatyczną, inkrementacyjną aktualizację silnika detekcji.
20. Rozwiązanie musi posiadać tylko jeden proces uruchamiany w pamięci, z którego korzystają wszystkie funkcje systemu (antywirus, antyspyware, metody heurystyczne).
21. Rozwiązanie musi posiadać funkcjonalność skanera UEFI, który chroni użytkownika poprzez wykrywanie i blokowanie zagrożeń, atakujących jeszcze przed uruchomieniem systemu operacyjnego.
22. Rozwiązanie musi posiadać ochronę antyspamową dla programu pocztowego Microsoft Outlook.
23. Zapora osobista rozwiązania musi pracować w jednym z czterech trybów:
    1. tryb automatyczny – rozwiązanie blokuje cały ruch przychodzący i zezwala tylko na połączenia wychodzące,
    2. tryb interaktywny – rozwiązanie pyta się o każde nowo nawiązywane połączenie,
    3. tryb oparty na regułach – rozwiązanie blokuje cały ruch przychodzący i wychodzący, zezwalając tylko na połączenia skonfigurowane przez administratora,
    4. tryb uczenia się – rozwiązanie automatycznie tworzy nowe reguły zezwalające na połączenia przychodzące i wychodzące. Administrator musi posiadać możliwość konfigurowania czasu działania trybu.
24. Rozwiązanie musi być wyposażona w moduł bezpiecznej przeglądarki.
25. Przeglądarka musi automatycznie szyfrować wszelkie dane wprowadzane przez Użytkownika.
26. Praca w bezpiecznej przeglądarce musi być wyróżniona poprzez odpowiedni kolor ramki przeglądarki oraz informację na ramce przeglądarki.
27. Rozwiązanie musi być wyposażone w zintegrowany moduł kontroli dostępu do stron internetowych.
28. Rozwiązanie musi posiadać możliwość filtrowania adresów URL w oparciu o co najmniej 140 kategorii i podkategorii.
29. Rozwiązanie musi zapewniać ochronę przed zagrożeniami 0-day.
30. W przypadku stacji roboczych rozwiązanie musi posiadać możliwość wstrzymania uruchamiania pobieranych plików za pośrednictwem przeglądarek internetowych, klientów poczty e-mail, z nośników wymiennych oraz wyodrębnionych z archiwum.

Ochrona serwera.

1. Rozwiązanie musi wspierać systemy Microsoft Windows Server 2012 i nowszych oraz Linux w tym co najmniej: RedHat Enterprise Linux (RHEL) 7,8 i 9, CentOS 7, Ubuntu Server (SLES) 15, Oracle Linux 8 oraz Amazon Linux.
2. Rozwiązanie musi zapewniać ochronę przed wirusami, trojanami, robakami i innymi zagrożeniami.
3. Rozwiązanie musi zapewniać wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor.
4. Rozwiązanie musi zapewniać możliwość skanowania dysków sieciowych typu NAS.
5. Rozwiązanie musi posiadać wbudowane dwa niezależne moduły heurystyczne – jeden wykorzystujący pasywne metody heurystyczne i drugi wykorzystujący aktywne metody heurystyczne oraz elementy sztucznej inteligencji. Rozwiązanie musi istnieć możliwość wyboru, z jaką heurystyka ma odbywać się skanowanie – z użyciem jednej lub obu metod jednocześnie.
6. Rozwiązanie musi wspierać automatyczną, inkrementacyjną aktualizację silnika detekcji.
7. Rozwiązanie musi posiadać możliwość wykluczania ze skanowania procesów.
8. Rozwiązanie musi posiadać możliwość określenia typu podejrzanych plików, jakie będą przesyłane do producenta, w tym co najmniej pliki wykonywalne, archiwa, skrypty, dokumenty.

Dodatkowe wymagania dla ochrony serwerów Windows:

1. Rozwiązanie musi posiadać możliwość skanowania plików i folderów, znajdujących się w usłudze chmurowej OneDrive.
2. Rozwiązanie musi posiadać system zapobiegania włamaniom działający na hoście (HIPS).
3. Rozwiązanie musi wspierać skanowanie magazynu Hyper-V.
4. Rozwiązanie musi posiadać funkcjonalność skanera UEFI, który chroni użytkownika poprzez wykrywanie i blokowanie zagrożeń, atakujących jeszcze przed uruchomieniem systemu operacyjnego.
5. Rozwiązanie musi zapewniać administratorowi blokowanie zewnętrznych nośników danych na stacji w tym przynajmniej: Pamięci masowych, optycznych pamięci masowych, pamięci masowych Firewire, urządzeń do tworzenia obrazów, drukarek USB, urządzeń Bluetooth, czytników kart inteligentnych, modemów, portów LPT/COM oraz urządzeń przenośnych.
6. Rozwiązanie musi automatyczne wykrywać usługi zainstalowane na serwerze i tworzyć dla nich odpowiednie wyjątki.
7. Rozwiązanie musi posiadać wbudowany system IDS z detekcją prób ataków, anomalii w pracy sieci oraz wykrywaniem aktywności wirusów sieciowych.
8. Rozwiązanie musi zapewniać możliwość dodawania wyjątków dla systemu IDS, co najmniej w oparciu o występujący alert, kierunek, aplikacje, czynność oraz adres IP.
9. Rozwiązanie musi posiadać ochronę przed oprogramowaniem wymuszającym okup za pomocą dedykowanego modułu.

Dodatkowe wymagania dla ochrony serwerów Linux:

1. Rozwiązanie musi pozwalać, na uruchomienie lokalnej konsoli administracyjnej, działającej z poziomu przeglądarki internetowej.
2. Lokalna konsola administracyjna nie może wymagać do swojej pracy, uruchomienia i instalacji dodatkowego rozwiązania w postaci usługi serwera Web.
3. Rozwiązanie musi działać w architekturze bazującej na technologii mikro-serwisów. Funkcjonalność ta musi zapewniać podwyższony poziom stabilności, w przypadku awarii jednego z komponentów rozwiązania, nie spowoduje to przerwania pracy całego procesu, a jedynie wymusi restart zawieszonego mikro-serwisu.

Szyfrowanie.

1. System szyfrowania danych musi wspierać instalację aplikacji klienckiej w środowisku Microsoft Windows 10/11 32-bit i 64-bit.
2. System szyfrowania musi wspierać zarządzanie natywnym szyfrowaniem w systemach macOS (FileVault).
3. Aplikacja musi posiadać autentykacje typu Pre-boot, czyli uwierzytelnienie użytkownika zanim zostanie uruchomiony system operacyjny. Musi istnieć także możliwość całkowitego lub czasowego wyłączenia tego uwierzytelnienia.
4. Aplikacja musi umożliwiać szyfrowanie danych na komputerach z UEFI.

Ochrona urządzeń mobilnych opartych o system Android.

1. Rozwiązanie musi zapewniać skanowanie wszystkich typów plików, zarówno w pamięci wewnętrznej, jak i na karcie SD, bez względu na ich rozszerzenie.
2. Rozwiązanie musi zapewniać co najmniej 2 poziomy skanowania: inteligentne i dokładne.
3. Rozwiązanie musi zapewniać automatyczne uruchamianie skanowania, gdy urządzenie jest w trybie bezczynności (w pełni naładowane i podłączone do ładowarki).
4. Rozwiązanie musi posiadać możliwość skonfigurowania zaufanej karty SIM.
5. Rozwiązanie musi zapewniać wysłanie na urządzenie komendy z konsoli centralnego zarządzania, która umożliwi:
   1. usunięcie zawartości urządzenia,
   2. przywrócenie urządzenie do ustawień fabrycznych,
   3. zablokowania urządzenia,
   4. uruchomienie sygnału dźwiękowego,
   5. lokalizację GPS.
   6. Rozwiązanie musi zapewniać administratorowi podejrzenie listy zainstalowanych aplikacji.
   7. Rozwiązanie musi posiadać blokowanie aplikacji w oparciu o:
   8. nazwę aplikacji,
   9. nazwę pakietu,
   10. kategorię sklepu Google Play,
   11. uprawnienia aplikacji,
   12. pochodzenie aplikacji z nieznanego źródła.

Ochrona serwera pocztowego MS Exchange.

1. Rozwiązanie musi wspierać instalację na systemach Microsoft Windows Server 2012 i nowszych.
2. Rozwiązanie musi zapewniać wsparcie dla systemów poczty Microsoft Exchange 2010/2013/2016/2019.
3. Rozwiązanie musi zapewniać wsparcie dla ról Mailbox, Edge, Hub.
4. Rozwiązanie musi skanować pocztę przychodzącą i wychodzącą na serwerze MS Exchange.
5. Rozwiązanie musi zapewnić skanowanie bezpośrednio w bazach danych Exchange przy pomocy VSAPI.
6. Rozwiązanie musi mieć możliwość tworzenia różnych reguł blokowania wiadomości w tym co najmniej po zdefiniowanym nadawcy, odbiorcy, temacie wiadomości, typie załącznika, rozmiarze załącznika, rozmiarze wiadomości, nagłówku wiadomości, na podstawie uzyskanego wyniku skanowania antyspamowego i antywirusowego, godzinie odbioru, obecności załącznika chronionego hasłem lub uszkodzonego archiwum.
7. Rozwiązanie musi posiadać wbudowany w oprogramowanie filtr antyspamowy odpowiedzialny za filtrowanie niechcianej poczty.
8. System antyspamowy ma być wyposażony przynajmniej w możliwość sprawdzania list RBL, DNSBL oraz mechanizm reputacji poczty.
9. Administrator musi mieć możliwość dodania własnych adresów list RBL oraz DSBL, z których będzie korzystać aplikacja.
10. Rozwiązanie ma posiadać mechanizm greylisting (szara lista).
11. Rozwiązanie musi zapewniać ochronę przed zagrożeniami 0-day.

Sandbox w chmurze.

1. Rozwiązanie musi zapewniać ochronę przed zagrożeniami 0-day.
2. Rozwiązanie musi wykorzystywać do działania chmurę producenta.
3. Rozwiązanie musi posiadać możliwość określenia jakie pliki mają zostać przesłane do chmury automatycznie, w tym archiwa, skrypty, pliki wykonywalne, możliwy spam, dokumenty oraz inne pliki typu .jar, .reg, .msi.
4. Administrator musi mieć możliwość zdefiniowania po jakim czasie przesłane pliki muszą zostać usunięte z serwerów producenta.
5. Administrator musi mieć możliwość zdefiniowania maksymalnego rozmiaru przesyłanych próbek.
6. Rozwiązanie musi pozwalać na utworzenie listy wykluczeń określonych plików lub folderów z przesyłania.
7. Po zakończonej analizie pliku, rozwiązanie musi przesyłać wynik analizy do wszystkich wspieranych produktów.
8. Administrator musi mieć możliwość podejrzenia listy plików, które zostały przesłane do analizy.
9. Rozwiązanie musi pozwalać na analizowanie plików, bez względu na lokalizacje stacji roboczej. W przypadku wykrycia zagrożenia, całe środowisko jest bezzwłocznie chronione.
10. Rozwiązanie nie może wymagać instalacji dodatkowego agenta na stacjach roboczych.
11. Rozwiązanie pozwala na wysłanie dowolnej próbki do analizy przez użytkownika lub administratora, za pomocą wspieranego produktu. Administrator musi móc podejrzeć jakie pliki zostały wysłane do analizy oraz przez kogo.
12. Przeanalizowane pliki muszą zostać odpowiednio oznaczone. Analiza pliku może zakończyć się z wynikiem:
    1. Czysty,
    2. Podejrzany,
    3. Bardzo podejrzany,
    4. Szkodliwy.
13. W przypadku stacji roboczych rozwiązanie musi posiadać możliwość wstrzymania uruchamiania pobieranych plików za pośrednictwem przeglądarek internetowych, klientów poczty e-mail, z nośników wymiennych oraz wyodrębnionych z archiwum.
14. W przypadku serwerów pocztowych rozwiązanie musi posiadać możliwość wstrzymania dostarczania wiadomości do momentu zakończenia analizy próbki.
15. Wykryte zagrożenia muszą być przeniesione w bezpieczny obszar kwarantanny, z której administrator może przywrócić dowolne pliki oraz utworzyć dla niej wyłączenia.

Ochrona usługi Microsoft 365.

1. Rozwiązanie musi obejmować ochroną usługi Microsoft, takie jak Exchange Online, Onedrive, Sharepoint oraz aplikację Teams.
2. Rozwiązanie musi posiadać możliwość dodania kilku tenantów usługi Micosoft 365.
3. Administrator musi mieć możliwość wskazania, które konto użytkownika będzie objęte ochroną.
4. Rozwiązanie musi być zarządzane za pomocą dowolnej przeglądarki internetowej z dowolnego miejsca w sieci.
5. Rozwiązanie musi być dostępne w języku polskim.
6. Konsola rozwiązania musi posiadać możliwość raportowania co najmniej:
   1. użytkowników, otrzymujących najwięcej spamu,
   2. użytkowników, otrzymujących najwięcej wiadomości typu „phishing”,
   3. użytkowników, otrzymujących największą ilość szkodliwego oprogramowania,
   4. kont użytkowników, które mogę być podejrzane.
7. Konsola rozwiązania musi posiadać funkcjonalność logowania zdarzeń z podziałem na dzienniki dla Exchange Online i Onedrive.
8. Dzienniki Exchange Online muszą posiadać funkcjonalność informowania co najmniej:
   1. jaka ilość wiadomości została przeskanowania,
   2. wynik skanowania poszczególnej wiadomości,
   3. czynność podjęta przez rozwiązanie.
9. Dzienniki Onedrive muszą posiadać funkcjonalność informowania co najmniej o: zagrożeniach, które zostały wykryte,
   1. na jakim koncie zostały wykryte,
   2. jakie zagrożenie zostało wykryte,
   3. podjętą czynność.
10. Rozwiązanie musi posiadać funkcjonalność kwarantanny, do której będą przenoszone zainfekowane obiekty z usługi Exchange Online oraz Onedrive.
11. Musi istnieć możliwość pobrania plików z kwarantanny w formie oryginalnego pliku i pliku zabezpieczonego hasłem.
12. Administrator musi posiadać możliwość przypisania konfiguracji, do dodanych do rozwiązania tenantów lub do poszczególnych grup i użytkowników.
13. Administrator musi posiadać możliwość konfiguracji rozwiązania w oparciu o co najmniej:
    1. wykorzystania do analizy mechanizmów chmurowych, tego samego producenta,
    2. wprowadzenia białych i czarnych list adresów ochrony Exchange’a Online,
    3. dodania znacznika do tematu wiadomości zakwalifikowanej jako SPAM i phishing.
14. Rozwiązanie musi zapewniać funkcję ochrony przed zagrożeniami 0-day.
15. Funkcja ochrony przed zagrożeniami 0-day musi wykorzystywać do działania chmurę producenta.
16. Funkcja ochrony przed zagrożeniami 0-day musi posiadać możliwość określenia jakie pliki mają zostać przesłane do chmury automatycznie, w tym archiwa, skrypty, pliki wykonywalne, możliwy spam, dokumenty oraz inne pliki typu .jar, .reg, .msi.
17. Administrator musi mieć możliwość zdefiniowania po jakim czasie przesłane pliki muszą zostać usunięte z serwerów producenta.
18. Rozwiązanie musi posiadać możliwość przesyłania powiadomień e-mail z funkcją wyboru preferowanego języka.

# Wyposażenie stanowisk pracowniczych - zakup stacji roboczych (8 szt.).

Minimalne parametry zestawu komputerowego:

1. Zestaw komputerowy musi być przeznaczony do zastosowań biurowych.
2. Procesor wielordzeniowy ze zintegrowanym układem graficznym osiągający w teście wydajności CPU PassMark Performance Test (https://www.cpubenchmark.net) z wynikiem aktualnym w okresie 30 dni przed terminem składania ofert co najmniej wynik 20 000 punktów. Zamawiający żąda załączenia do oferty przedmiotowego środka dowodowego określonego w SWZ potwierdzającego spełnienie przez oferowany procesor żądanej przez Zamawiającego wydajności.
3. Pamięć operacyjna min. 16 GB w najnowszej technologii oferowanej przez producenta komputera, przy czym komputer musi posiadać min. 1 niezajęte złącze do rozbudowy i obsługiwać do 32GB pamięci.
4. Pamięć masowa – dysk w technologii SSD min. 512 GB z interfejsem M.2.
5. Karta graficzna zintegrowana, z możliwością dynamicznego przydzielania pamięci w obrębie pamięci systemowej.
6. Zintegrowana karta dźwiękowa musi obsługiwać dźwięk 24bit HD.
7. Obudowa musi zapewniać bezpośrednie podłączenie co najmniej dwóch urządzeń USB oraz mikrofonu z przodu.
8. Komputer musi być wyposażony w zasilacz wewnętrzny o mocy maksymalnej nieprzekraczającej 300W.
9. Wyposażenie minimalne: nieusuwalne 1xDP i 1xHDMI lub 2xDP, nieusuwalne co najmniej 6 portów USB, w tym co najmniej 2 x USB 3.0 na panelu przednim komputera, nieusuwalny czytnik kart pamięci, napęd optyczny DVD-RW; klawiatura USB w układzie polski programisty i mysz bezprzewodowa (dwuprzyciskowa, rolka/scroll jako trzeci przycisk); nośnik z systemem operacyjnym i sterownikami; głośnik, 1x wyjście słuchawkowe oraz 1x wejście mikrofonowe na panelu przednim obudowy (dopuszcza się jedno wspólne złącze słuchawkowo – mikrofonowe), karta sieciowa 10/100/1000 Mbit/s Ethernet RJ 45 wspierająca obsługę WoL.
10. Oferowany komputer musi zostać dostarczony z licencją oprogramowania systemu operacyjnego klasy Microsoft Windows 11 PRO lub równoważny. Za równoważny system operacyjny Zamawiający uzna system spełniający następujące minimalne parametry: Możliwość dokonywania aktualizacji i poprawek systemu przez Internet; możliwość dokonywania uaktualnień sterowników urządzeń przez Internet – witrynę producenta systemu; Darmowe aktualizacje w ramach wersji systemu operacyjnego przez Internet (niezbędne aktualizacje, poprawki, biuletyny bezpieczeństwa muszą być dostarczane bez dodatkowych opłat) – wymagane podanie nazwy strony serwera WWW; Internetowa aktualizacja zapewniona w języku polskim; Wbudowana zapora internetowa (firewall) dla ochrony połączeń internetowych; zintegrowana z systemem konsola do zarządzania ustawieniami zapory i regułami IPSec v4 i v6; Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, przeglądarka internetowa, pomoc, komunikaty systemowe; Wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (np.: drukarek, urządzeń sieciowych, standardów USB, Plug&Play, Wi-Fi); Możliwość zdalnej automatycznej instalacji, konfiguracji, administrowania oraz aktualizowania systemu; Zabezpieczony hasłem hierarchiczny dostęp do systemu, konta i profile użytkowników zarządzane zdalnie; praca systemu w trybie ochrony kont użytkowników; Zintegrowany z systemem moduł wyszukiwania informacji (plików różnego typu) dostępny z kilku poziomów: poziom menu, poziom otwartego okna systemu operacyjnego; system wyszukiwania oparty na konfigurowalnym przez użytkownika module indeksacji zasobów lokalnych; Zintegrowane z systemem operacyjnym narzędzia zwalczające złośliwe oprogramowanie; aktualizacje dostępne u producenta nieodpłatnie bez ograniczeń czasowych; Wbudowany system pomocy w języku polskim; System operacyjny powinien być wyposażony w możliwość przystosowania stanowiska dla osób niepełnosprawnych (np. słabo widzących); Możliwość zarządzania stacją roboczą poprzez polityki – przez politykę rozumiemy zestaw reguł definiujących lub ograniczających funkcjonalność systemu lub aplikacji; System posiadać powinien narzędzia służące do administracji, do wykonywania kopii zapasowych polityk i ich odtwarzania oraz generowania raportów z ustawień polityk; Zdalna pomoc i współdzielenie aplikacji – możliwość zdalnego przejęcia sesji zalogowanego użytkownika celem rozwiązania problemu z komputerem; Graficzne środowisko instalacji i konfiguracji; Zarządzanie kontami użytkowników sieci oraz urządzeniami sieciowymi tj. drukarki, modemy, woluminy dyskowe, usługi katalogowe; Możliwość przywracania plików systemowych.
11. Oferowany komputer musi zostać dostarczony z bezterminową licencją oprogramowania pakietu biurowego klasy Microsoft Office 2021 lub równoważny. Za równoważny system operacyjny Zamawiający uzna system spełniający następujące minimalne parametry:
    1. Dostawa pełnej polskiej wersji językowej interfejsu użytkownika, w tym także systemu interaktywnej pomocy w języku polskim. Pakiet powinien mieć system aktualizacji darmowych poprawek bezpieczeństwa, przy czym komunikacja z użytkownikiem powinna odbywać się w języku polskim. Dostępność w Internecie na stronach producenta biuletynów technicznych, w tym opisów poprawek bezpieczeństwa, w języku polskim, a także telefonicznej pomocy technicznej producenta pakietu biurowego świadczonej w języku polskim w dni robocze w godzinach pracy Urzędu – cena połączenia nie większa niż cena połączenia lokalnego. Publicznie znany cykl życia przedstawiony przez producenta dotyczący rozwoju i wsparcia technicznego – w szczególności w zakresie bezpieczeństwa co najmniej 5 lat od daty zakupu. Możliwość dostosowania pakietu aplikacji biurowych do pracy dla osób niepełnosprawnych np. słabo widzących, zgodnie z wymogami Krajowych Ram Interoperacyjności (WCAG 2.0).
    2. Zintegrowany pakiet aplikacji biurowych musi zawierać co najmniej:

* edytor tekstów,
* arkusz kalkulacyjny,
* narzędzie do przygotowania i prowadzenia prezentacji,
* narzędzie do zarządzania informacją osobistą (pocztą elektroniczną, kalendarzem, kontaktami i zadaniami).
  1. Edytor tekstów musi umożliwiać co najmniej:
* Edycję i formatowanie tekstu w języku polskim wraz z obsługą języka polskiego w zakresie sprawdzania pisowni i poprawności gramatycznej oraz funkcjonalnością słownika wyrazów bliskoznacznych i autokorekty.
* Wstawianie oraz formatowanie tabel.
* Wstawianie oraz formatowanie obiektów graficznych.
* Wstawianie wykresów i tabel z arkusza kalkulacyjnego (wliczając tabele przestawne).
* Automatyczne numerowanie rozdziałów, punktów, akapitów, tabel i rysunków.
* Automatyczne tworzenie spisów treści.
* Formatowanie nagłówków i stopek stron.
* Śledzenie i porównywanie zmian wprowadzonych przez użytkowników w dokumencie.
* Nagrywanie, tworzenie i edycję makr automatyzujących wykonywanie czynności.
* Określenie układu strony (pionowa/pozioma).
* Wydruk dokumentów.
* Wykonywanie korespondencji seryjnej bazując na danych adresowych pochodzących z arkusza kalkulacyjnego i z narzędzia do zarządzania informacją prywatną.
* Zabezpieczenie dokumentów hasłem przed odczytem oraz przed wprowadzaniem modyfikacji.
* Wymagana jest dostępność do oferowanego edytora tekstu bezpłatnych narzędzi umożliwiających podpisanie podpisem elektronicznym pliku z zapisanym dokumentem przy pomocy certyfikatu kwalifikowanego zgodnie z wymaganiami obowiązującego w Polsce prawa.
  1. Arkusz kalkulacyjny musi umożliwiać co najmniej:
* Tworzenie raportów tabelarycznych.
* Tworzenie wykresów liniowych (wraz linią trendu), słupkowych, kołowych.
* Tworzenie arkuszy kalkulacyjnych zawierających teksty, dane liczbowe oraz formuły przeprowadzające operacje matematyczne, logiczne, tekstowe, statystyczne oraz operacje na danych finansowych i na miarach czasu.
* Tworzenie raportów z zewnętrznych źródeł danych (inne arkusze kalkulacyjne, bazy danych zgodne z ODBC, pliki tekstowe, pliki XML, webservice).
* Obsługę kostek OLAP oraz tworzenie i edycję kwerend bazodanowych i webowych.
* Narzędzia wspomagające analizę statystyczną i finansową, analizę wariantową i rozwiązywanie problemów optymalizacyjnych.
* Tworzenie raportów tabeli przestawnych umożliwiających dynamiczną zmianę wymiarów oraz wykresów bazujących na danych z tabeli przestawnych.
* Wyszukiwanie i zamianę danych.
* Wykonywanie analiz danych przy użyciu formatowania warunkowego.
* Nazywanie komórek arkusza i odwoływanie się w formułach po takiej nazwie.
* Nagrywanie, tworzenie i edycję makr automatyzujących wykonywanie czynności.
* Formatowanie czasu, daty i wartości finansowych z polskim formatem.
* Zapis wielu arkuszy kalkulacyjnych w jednym pliku.
* Zabezpieczenie dokumentów hasłem przed odczytem oraz przed wprowadzaniem modyfikacji.
  1. Narzędzie do przygotowywania i prowadzenia prezentacji musi umożliwiać co najmniej:
* Przygotowywanie prezentacji multimedialnych, które mogą być prezentowanie przy użyciu projektora multimedialnego.
* Drukowanie w formacie umożliwiającym robienie notatek.
* Zapisanie jako prezentacja tylko do odczytu.
* Nagrywanie narracji i dołączanie jej do prezentacji.
* Opatrywanie slajdów notatkami dla prezentera.
* Umieszczanie i formatowanie tekstów, obiektów graficznych, tabel, nagrań dźwiękowych i wideo.
* Umieszczanie tabel i wykresów pochodzących z arkusza kalkulacyjnego.
* Odświeżenie wykresu znajdującego się w prezentacji po zmianie danych w źródłowym arkuszu kalkulacyjnym.
* Możliwość tworzenia animacji obiektów i całych slajdów.
* Prowadzenie prezentacji w trybie prezentera, gdzie slajdy są widoczne na jednym monitorze lub projektorze, a na drugim widoczne są slajdy i notatki prezentera.
  1. Narzędzie do zarządzania informacją prywatną (pocztą elektroniczną, kalendarzem, kontaktami i zadaniami) musi umożliwiać:
* Pobieranie i wysyłanie poczty elektronicznej z serwera pocztowego.
* Przechowywanie wiadomości na serwerze lub w lokalnym pliku tworzonym z zastosowaniem efektywnej kompresji danych.
* Filtrowanie niechcianej poczty elektronicznej (SPAM) oraz określanie listy zablokowanych i bezpiecznych nadawców.
* Tworzenie katalogów, pozwalających katalogować pocztę elektroniczną.
* Automatyczne grupowanie poczty o tym samym tytule.
* Tworzenie reguł przenoszących automatycznie nową pocztę elektroniczną do określonych katalogów bazując na słowach zawartych w tytule, adresie nadawcy i odbiorcy.
* Oflagowanie poczty elektronicznej z określeniem terminu przypomnienia, oddzielnie dla nadawcy i adresatów.
* Mechanizm ustalania liczby wiadomości, które mają być synchronizowane lokalnie.
* Zarządzanie kalendarzem.
* Udostępnianie kalendarza innym użytkownikom z możliwością określania uprawnień użytkowników.
* Przeglądanie kalendarza innych użytkowników.
* Zapraszanie uczestników na spotkanie, co po ich akceptacji powoduje automatyczne wprowadzenie spotkania w ich kalendarzach.
* Zarządzanie listą zadań.
* Zlecanie zadań innym użytkownikom.
* Zarządzanie listą kontaktów.
* Udostępnianie listy kontaktów innym użytkownikom.
* Przeglądanie listy kontaktów innych użytkowników.
* Możliwość przesyłania kontaktów innym użytkowników.

1. Komputer musi zostać wyposażony w monitor o parametrach minimalnych:
   1. ekran matowy typu LED o przekątnej co najmniej 27”;
   2. jasność przynajmniej 250cd/m2; kontrast typowy przynajmniej 1000:1,
   3. rozdzielczość co najmniej 1920x1080;
   4. wbudowane głośniki bądź montowana listwa głośnikowa,
   5. możliwość obrotu ekranu w osi pion i poziom oraz podnoszenia ekranu,
   6. złącza wbudowane fabrycznie: nieusuwalne 1xDP i 1xHDMI lub 2xDP (zgodne ze złączem oferowanym w jednostce centralnej),
   7. złącze linki antykradzieżowej.
2. Dokumenty potwierdzające jakość produktu i sposobu jego wykonania: Certyfikat ISO 9001 lub inny równoważny dokument poświadczający, że producent jednostki centralnej oraz monitora opracował, wdrożył i certyfikował system zarządzania jakością; Certyfikat ISO 50001 lub inny równoważny dokument poświadczający, że producent jednostki centralnej oraz monitora posiada system zarządzania energią, zmniejszający zużycie energii, wpływy na środowisko i zwiększający rentowność; Deklaracja zgodności CE lub inny równoważny dokument poświadczający, że oferowana jednostka centralna oraz monitor spełniają wszystkie zasadnicze wymagania zawarte w poszczególnych dyrektywach nowego podejścia przewidujących oznakowanie CE; Potwierdzenie spełnienia kryteriów środowiskowych, w tym zgodności z dyrektywą RoHS Unii Europejskiej o eliminacji substancji niebezpiecznych dla jednostki centralnej i monitora. Zamawiający żąda załączenia do oferty przedmiotowych środków dowodowych - dokumentów potwierdzających spełnienie przez oferowane urządzenia i jego/ich producenta/producentów w zakresie określonym powyżej.
3. Gwarancja: min. 60 miesięcy gwarancji producenta na jednostkę centralną i monitor świadczona na miejscu u użytkownika końcowego. Czas reakcji serwisu - do końca następnego dnia roboczego. Serwis urządzeń musi byś realizowany przez producenta lub autoryzowanego partnera serwisowego producenta. Dostęp do aktualnych sterowników zainstalowanych w komputerze urządzeń, realizowany poprzez podanie identyfikatora klienta lub modelu komputera lub numeru seryjnego komputera, na dedykowanej przez producenta stronie internetowej umożliwiającej zgłaszanie awarii lub usterek oraz sprawdzenie okresu gwarancji jednostki centralnej i monitora. Czas reakcji serwisu - do końca następnego dnia roboczego. Serwis urządzeń musi byś realizowany przez producenta lub autoryzowanego partnera serwisowego producenta lub Wykonawcę. W okresie gwarancji uszkodzone dyski pozostają u Zamawiającego.

# Wyposażenie stanowisk pracowniczych - zakup urządzenia wielofunkcyjnego (1 szt.).

Minimalne parametry urządzenia wielofunkcyjnego:

1. Urządzenie musi zapewniać możliwość drukowania, skanowania i kopiowania. Urządzenie wolnostojące, wyposażone w podstawę na kółkach w celu przemieszczania.
2. Technologia druku: czarno-biały i kolorowy druk laserowy.
3. Format druku i skanu: min. A3.
4. Druk i skan dwustronny.
5. W zestawie 3 podajniki: min. jeden automatyczny podajnik dokumentów na 200 arkuszy o gramaturze 80 g/m2; min. dwa o pojemności min. 550 ark. (80g/m2); min. 1 obsługujący koperty oraz format papieru A6R-A3.
6. Wbudowany wewnętrzny dysk twardy o pojemności min. 250 GB.
7. Rozdzielczość druku mono i kolor: min. 1200x1200 dpi.
8. Możliwość skanowania w kolorze.
9. Optyczna rozdzielczość skanowania: min. 600x600 dpi.
10. Skanowanie do e-mail oraz do plików w formacie JPEG, TIFF, PDF. Wbudowany moduł OCR bez limitu stron i licencji pozwalający skanować do formatów Word, PowerPoint, Przeszukiwalnego PDF.
11. Panel sterujący urządzeniem z wyświetlaczem LCD.
12. Obsługa przez urządzenie szyfrowanego protokołu TLS 1.3.
13. Obsługa rozmiarów papieru: A3, A4, A5, A6.
14. Obsługa papieru o gramaturze do 300 g/m².
15. Druk w sieci LAN.
16. Min. 2 x USB.
17. Urządzenie powinno umożliwiać zszywanie dokumentów w pozycji róg lub podwójne.
18. Pojemność zszywacza nie mniej niż 40 arkuszy A4 (80g/m2) oraz minimum 30 arkuszy A3 (80g/m2).
19. W zestawie oryginalne materiały eksploatacyjne w postaci zestawu tonerów umożliwiające wydruk 50 000 stron A4 w kolorze zgodnie z deklarowaną wydajnością tonera określoną przez producenta tonera.
20. Dokumenty potwierdzające jakość produktu i sposobu jego wykonania: Deklaracja zgodności CE lub inny równoważny dokument poświadczający, że oferowane urządzenie spełnia wszystkie zasadnicze wymagania zawarte w poszczególnych dyrektywach nowego podejścia przewidujących oznakowanie CE. Zamawiający żąda załączenia do oferty przedmiotowych środków dowodowych - dokumentów potwierdzających spełnienie przez oferowane urządzenie wymagań w zakresie określonym powyżej.
21. Co najmniej 36 miesięcy gwarancji producenta realizowanej w siedzibie Zamawiającego.