Mogielnica, 03.10.2022

Gmina Mogielnica
ul. Rynek 1
05-640 Mogielnica

OGŁOSZENIE

Burmistrz Gminy i Miasta Mogielnica w związku z realizacją projektu **„Cyfrowa Gmina"** zaprasza do składania ofert na:

ZAKUP i DOSTAWA SPRZĘTU KOMPUTEROWEGO I OPROGRAMOWANIA

I. Opis przedmiotu zamówienia:

Przedmiotem zamówienia jest **zakup i dostawa niżej wymienionego sprzętu komputerowego oraz oprogramowania** o parametrach:

1. Dwustronny skaner dokumentów – szt. 2

Połączenie: Interfejs USB Hi-Speed USB 2.0; Waga Max 2,6kg
Zużycie energii: Praca 21W, Tryb gotowości 4,7W, Tryb uśpienia 0,8W, Wyłączone 0,1W; Moc dźwięku Max 50dB
Specyfikacje nośników min.
Rozmiary nośników podajnika ADF: Min. A4, A5, A6, B5, B6, Executive, Legal, Letter
Typy nośników podajnika ADF: Papier błyszczący, Papier do drukarek atramentowych, Papier ekologiczny, Papier standardowy, Gruby papier, Cienki papier
Gramatura nośników podajnika ADF: Min. 50-209gsm
Rozmiary nośników podajnika ADF: Min Szerokość: 51-215.9mm, Długość: 51-355.6mm.
Skanowanie
Skanowanie 2-stronne: Skanowanie dwustronne
ADF: Min. 50
Szybkość skanowania kolorowego A4: Min. 35 str./min
Głębia kolorów: Min. 48 bity
Sterowniki:TWAIN, WIA, SANE, ICA
Interpolowana rozdzielczość skanowania: Min. 1200 x 1200 dpi
Czujnik papieru: Tak
Rozdzielczość skanowania z podajnika ADF: Min. 600 x 600
Skanuj do: Obraz, plik, OCR, USB,
Skala szarości:256
Okres gwarancji w miesiącach minimum: 36 miesięcy
Czas naprawy to następny dzień roboczy
Naprawy realizowane na miejscu w siedzibie Klienta

2. **Serwer NAS – szt.1**

Typ urządzenia Serwer NAS, **Obudowa** Rack 1U, **Procesor** Czterordzeniowy procesor o taktowaniu 2,2 GHz osiągający w teście PassMark na sierpień 2022 co najmniej 4 580 punktów, **Sprzętowy mechanizm szyfrowania** Tak (AES-NI), **Pamięć RAM** min. 2 GB pamięci ECC SODIMM z możliwością rozszerzenia do min. 32 GB, **Możliwości rozbudowy** Sprzęt powinien być wyposażony w min. 4 kieszenie na dyski twarde typu hot-swap z możliwością rozszerzenia do 8 dysków łącznie przy użyciu dodatkowych jednostek rozszerzających podłączanych do jednostki głównej za pomocą portu eSATA, **Porty zewnętrzne** Minimum: - 2 porty USB 3.2.1, - 1 port eSATA (jako gniazdo rozszerzenia), **Porty sieciowe** Minimum: 4 porty 1GbE RJ45 (z obsługą funkcji Link Aggregation / przełączania awaryjnego), **Funkcja Wake on LAN/WAN** Tak, **Gniazdo rozszerzeń** PCIe 2.0 Min. 1x 4-liniowe gniazdo x8 gen. 3, **Wentylator obudowy** Min. 3 wentylatory (40 × 40 × 20 mm), **Obsługiwane protokoły sieciowe** Min. SMB1 (CIFS), SMB2, SMB3, NFSv3, NFSv4, NFSv4.1, NFS Kerberized sessions, iSCSI, HTTP, HTTPs, FTP, SNMP, LDAP, CalDAV, **Obsługiwane systemy plików** Min.: - Wewnętrzny: Btrfs, ext4, - Zewnętrzny: Btrfs, ext4, ext3, FAT, NTFS, HFS+, exFAT, **Zarządzanie pamięcią masową** - Maksymalny rozmiar pojedynczego wolumenu: 108 TB, - Minimalny liczba wewnętrznych wolumenów: 64, - Minimalny liczba obiektów iSCSI Target: 128, - Minimalny liczba jednostek iSCSI LUN: 256, - Obsługa klonowania/migawek jednostek iSCSI LUN, **Obsługiwane typy macierzy RAID** Min. SHR, Basic, JBOD, RAID 0, RAID 1, RAID 5, RAID 6, RAID 10, **Funkcja udostępniania plików** - Minimalna liczba kont użytkowników: 2 048, - Minimalna liczba grup użytkowników: 256, - Minimalna liczba folderów współdzielonych: 512, -Minimalna liczba jednoczesnych połączeń CIFS/AFP/NFS/FTP: 500* *Liczba jednoczesnych połączeń może zostać zwiększona do 2 000 po zainstalowaniu co najmniej 8 GB pamięci RAM. **Uprawnienia** listy kontroli dostępu systemu Windows® (ACL) i aplikacji, **Wirtualizacja** Obsługa VMware vSphere with VAAI, Microsoft Hyper-V®, Citrix®, OpenStack® 2, **Usługa katalogowa** Integracja z usługami Windows® AD, logowanie użytkowników domeny przez protokoły SMB/NFS/AFP/FTP lub aplikację File Station, integracja z LDAP, **Bezpieczeństwo** Zapora, szyfrowany folder współdzielony, szyfrowanie SMB, FTP przez SSL/TLS, SFTP, rsync przez SSH, automatyczne blokowanie logowania, obsługa Let's Encrypt, HTTPS (dostosowywane mechanizmy szyfrowania) Obsługiwane przeglądarki Google Chrome®, Firefox®, Microsoft Edge®, Safari® 13 i nowsze oraz Safari (iOS 13.0 i nowsze) na urządzeniach iPad, Chrome (Android™ 11.0 i nowsze) na tabletach, **Oprogramowanie** - Urządzenie musi umożliwiać utworzenie przestrzeni dyskowej w oparciu o nowoczesny system plików, który będzie zapewniał obsługę migawek, generowania sum kontrolnych CRC a także lustrzanych kopii metadanych aby zapewnić całkowitą integralność danych biznesowych. Dodatkowo wspomniany system musi wspierać ustawienie limitu dla folderów współdzielonych oraz szybkie klonowanie całych folderów współdzielonych, -Oprogramowanie zarządzające serwerem NAS musi zapewnić darmowe, kompleksowe rozwiązanie do tworzenia kopii zapasowych przeznaczone dla heterogenicznych środowisk IT, umożliwiające zdalne zarządzanie i monitorowanie ochrony komputerów, serwerów i maszyn wirtualnych na jednym, centralnym, przyjaznym dla administratora interfejsie. Ponadto gromadzone dane na urządzeniu mają mieć możliwość replikacji jako lokalne kopie zapasowe, sieciowe kopie zapasowe i kopie zapasowe danych w chmurach publicznych przy użyciu darmowego narzędzia instalowanego z Centrum Pakietów, - Wymaga się zapewnienia darmowej aplikacji do realizacji chmury prywatnej bez opłat cyklicznych, która będzie posiadała wygodną konsolę administratora zarządzaną z GUI a także agenty na urządzenia PC/MAC oraz aplikację mobilną na Android/iOS. Usługa powinna umożliwiać udostępnianie zasobów serwera NAS, synchronizację i tworzenie kopii zapasowych podłączonych urządzeń a także wspierać algorytm Intelliversioning. Ponadto

omawiana usługa powinna umożliwiać pracę z dokumentami biurowymi (edytor tekstowy, arkusz kalkulacyjny, pokaz slajdów) i wpierać wersjonowanie oraz edycję tworzonych plików office w czasie rzeczywistym, -Urządzenie musi umożliwiać pracę w trybie klastra wysokiej dostępności (HA) aby zapewnić nieprzerwany, natychmiastowy dostęp do zasobów bez widocznych zmian w użytkowaniu (konfiguracja jako jeden spójny system). Wszystkie dane z powodzeniem zapisane na serwerze aktywnym będą na bieżąco kopiowane do serwera pasywnego zapewniając replikację w czasie rzeczywistym i dostęp do danych oraz usług w przypadku uszkodzenia jednostki aktywnej dając gwarancję ciągłości pracy. 3 Utworzenie klastra HA ma się opierać o 2 identyczne urządzenia,
Dyski - urządzenie wyposażone w minimum 2 dyski 6TB o łącznej pojemności 12TB przeznaczone do pracy w urządzeniach NAS.
Szyny - dedykowane szyny rack
Okres gwarancji w miesiącach minimum: 36 miesięcy
Czas naprawy to następny dzień roboczy
Naprawy realizowane na miejscu w siedzibie Klienta

3. **Zapora UTM - szt.1**

Wymagania Ogólne
Dostarczony system bezpieczeństwa musi zapewniać wszystkie wymienione poniżej funkcje sieciowe i bezpieczeństwa niezależnie od dostawcy łącza. Dopuszcza się aby poszczególne elementy wchodzące 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 3 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 5 portami Gigabit Ethernet RJ-45.

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 20 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 700 tys. jednoczesnych połączeń oraz 35 tys. nowych połączeń na sekundę.
2. Przepustowość Stateful Firewall: nie mniej niż 5 Gbps dla pakietów 512 B.
3. Przepustowość Firewall z włączoną funkcją Kontroli Aplikacji: nie mniej niż 990 Mbps.
4. Wydajność szyfrowania IPSec VPN nie mniej niż 4,4 Gbps.
5. Wydajność skanowania ruchu w celu ochrony przed atakami (zarówno client side jak i server side w ramach modułu IPS) dla ruchu Enterprise Traffic Mix - minimum 1 Gbps.
6. Wydajność skanowania ruchu typu Enterprise Mix z włączonymi funkcjami: IPS, Application Control, Antywirus - minimum 600 Mbps.
7. Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL dla ruchu http – minimum 310 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 Stateful Inspection.
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 - Intrusion Prevention System.
6. Kontrola stron WWW.
7. Kontrola zawartości poczty – Antyspam dla protokołów SMTP, POP3.
8. Zarządzanie pasmem (QoS, Traffic shaping).
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 także dla protokołu HTTP/2.
12. Funkcja lokalnego serwera DNS ze wsparciem dla DNS over TLS (DoT) oraz DNS over HTTPS (DoH) z możliwością filtrowania zapytań DNS na lokalnym serwerze DNS jak i w ruchu przechodzącym przez system

Polityki, Firewall

13. Polityka Firewall musi uwzględniać adresy IP, użytkowników, protokoły, usługi sieciowe, aplikacje lub zbiory aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń.
14. 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.

15. W ramach systemu musi istnieć możliwość tworzenia wydzielonych stref bezpieczeństwa np. DMZ, LAN, WAN.
16. Możliwość wykorzystania w polityce bezpieczeństwa zewnętrznych repozytoriów zawierających: kategorie url, adresy IP, nazwy domenowe, hash'e złośliwych plików.
17. Element systemu realizujący funkcję Firewall musi integrować się z następującymi rozwiązaniami SDN w celu dynamicznego pobierania informacji o zainstalowanych maszynach wirtualnych po to aby użyć ich przy budowaniu polityk kontroli dostępu.
    - Amazon Web Services (AWS).
    - Microsoft Azure
    - Google Cloud Platform (GCP).
    - OpenStack.
    - VMware NSX.

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/Counter Mode(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.
    - Producent rozwiązania musi dostarczać oprogramowanie klienckie VPN, które umożliwia realizację połączeń IPSec VPN lub SSL VPN.

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.

Funkcje SD-WAN

1. System powinien umożliwiać wykorzystanie protokołów dynamicznego routingu przy konfiguracji równoważenia obciążenia do łączy WAN.
2. Reguły SD-WAN powinny umożliwiać określenie aplikacji jako argumentu dla kierowania ruchu.

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.

Ochrona przed malware

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.
5. System musi umożliwiać usuwanie aktywnej zawartości plików PDF oraz Microsoft Office bez konieczności blokowania transferu całych plików.
6. Możliwość wykorzystania silnika sztucznej inteligencji AI wytrenowanego przez laboratoria producenta.

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 5000 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 2000 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. Funkcja Safe Search – przeciwdziałająca pojawieniu się niechcianych treści w wynikach wyszukiwarek takich jak: Google, oraz Yahoo.
6. Administrator musi mieć możliwość definiowania komunikatów zwracanych użytkownikowi dla różnych akcji podejmowanych przez moduł filtrowania.
7. W ramach systemu musi istnieć możliwość określenia, dla których kategorii url lub wskazanych url - system nie będzie dokonywał inspekcji szyfrowanej komunikacji.

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.
4. Uwierzytelnianie w oparciu o protokół SAML w politykach bezpieczeństwa systemu dotyczących ruchu HTTP.

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.
7. Element systemu realizujący funkcję firewall musi umożliwiać wykonanie szeregu zmian przez administratora w CLI lub GUI, które nie zostaną zaimplementowane zanim nie zostaną zatwierdzone.

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 ICSA lub EAL4 dla funkcji Firewall.

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

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 zapewniać również dostęp do aktualizacji oprogramowania oraz wsparcie techniczne w trybie 24x7. Wykonawca musi zapewnić pierwszą linię wsparcia w języku polskim trybie 8x5. W celu realizacji wymogu wymagane jest posiadanie co najmniej dwóch inżynierów z aktualnym certyfikatem producenta oferowanego rozwiązania (jeżeli

producent oferowanego rozwiązania stosuje stopniowy system certyfikacji to co najmniej jeden z inżynierów musi posiadać najwyższy stopień certyfikacji) oraz ISO 9001 w zakresie serwisowania urządzeń informatycznych. Wszystkie certyfikaty należy dołączyć do oferty. Zamawiający dopuszcza, aby usługę wsparcia świadczył autoryzowany dystrybutor zaoferowanego urządzenia, ale wtedy wraz z ofertą należy dostarczyć oświadczenie tego dystrybutora o gotowości świadczenia takiego wsparcia na rzecz Zamawiającego wraz z zakresem tego wsparcia.
Pakiet wsparcia posprzedażowego rocznie za urządzenie w zakresie:

- wsparcie techniczne certyfikowanych inżynierów (Fortinet NSE4 – NSE8)
- system helpdesk z historią ticketu oraz wszystkich zrealizowanych zgłoszeń
- certyfikacja ISO 9001
- pomoc przy rejestracji urządzeń
- zakładanie zgłoszeń serwisowych u producenta
- pomoc w procesie realizacji naprawy i wymiany urządzeń w ramach gwarancji producenta
- doradztwo w zakresie konfiguracji
- podwyższony priorytet obsługi zgłoszeń
- możliwość zmiany priorytetu zgłoszenia w systemie producenta
- zdalna rekonfiguracja urządzenia (połączenie szyfrowane, do 10 zgłoszeń)
- szkolenie z konfiguracji urządzeń dla 1 osoby

4. Serwer wraz z systemem operacyjnym – szt.1

Obudowa: Typu RACK, wysokość nie więcej niż 2U; **Szyny**: umożliwiające wysunięcie serwera z szafy stelażowej; **Płyta główna:** Dwuprocesorowa; Wyprodukowana i zaprojektowana przez producenta serwera; 6 złącz PCI Express generacji 3 w tym: 3 złącza o prędkości x16, 3 złącza o prędkości x8; 12 gniazd pamięci RAM; Obsługa minimum 768GB pamięci RAM; Możliwość zainstalowania modułu TPM; Wsparcie dla technologii: Memory Scrubbing, SDDC,Advanced ECC; **Procesory** jeden procesor 8-rdzeniowy, architektura x86_64, Taktowanie bazowe 2,1GHz, zapewniający wydajność min. 11100 pkt. (dla pojedynczego procesora) w teście Passmark CPU Mark, znajdujący się na liście https://www.cpubenchmark.net/cpu_list.php (wynik na dzień 25.05.2022); **Pamięć RAM** 64 GB pamięci RAM, DDR4 Registered, 2933Mhz;**Dyski twarde** Minimum 8 wnęk dla dysków twardych Hotplug 2,5"; Zainstalowane 2 dyski SSD SATA 960GB HOT PLUG 2.5";**Kontrolery LAN** Trwale zintegrowana karta LAN, nie zajmująca żadnego z dostępnych slotów PCI Express, wyposażona minimum w interfejsy: 2x 1Gbit Base-T ze wsparciem iSCSI i iSCSI boot; **Kontrolery I/O** Kontroler RAID dla wewnętrznych dysków twardych posiadający obsługujący poziomy RAID: 0,1,10,5; **Porty** Zintegrowana karta graficzna ze złączem VGA; 2 porty USB 3.0 na panelu przednim; 1 port USB 3.0 wewnętrzny; 4 porty USB 3.0 dostępne z tyłu serwera; 1 port serial/RS232 – możliwość rozbudowy; Ilość dostępnych złącz USB nie może być osiągnięta poprzez stosowanie zewnętrznych przejściówek, rozgałęziaczy czy dodatkowych kart rozszerzeń zajmujących jakikolwiek slot PCI Express i/lub USB serwera; **Zasilanie, chłodzenie** Dwa zasilacze hotplug o sprawności 94% (tzw klasa Platinum) o mocy 450W, redundancja zasilania; Redundantne wentylatory; **Zarządzanie** Wbudowane diody informacyjne lub wyświetlacz informujące o stanie serwera; Zintegrowany z płytą główną serwera kontroler sprzętowy zdalnego zarządzania zgodny z IPMI 2.0 o funkcjonalnościach: Niezależny od systemu operacyjnego, sprzętowy kontroler umożliwiający pełne zarządzanie, zdalny restart serwera; Dedykowana karta LAN 1 Gb/s, dedykowane złącze RJ-45 do komunikacji wyłącznie z kontrolerem zdalnego zarządzania z możliwością przeniesienia tej komunikacji na inną kartę sieciową współdzieloną z systemem operacyjnym; Dostęp poprzez przeglądarkę Web, SSH; Zarządzanie mocą i jej zużyciem oraz monitoring zużycia energii; Zarządzanie alarmami (zdarzenia poprzez SNMP) Możliwość

przejęcia konsoli tekstowej, Możliwość zarządzania przez 6 administratorów jednocześnie, Opcjonalne przekierowanie konsoli graficznej na poziomie sprzętowym oraz możliwość montowania zdalnych napędów i ich obrazów na poziomie sprzętowym (cyfrowy KVM); Obsługa serwerów proxy (autentykacja); Obsługa VLAN, Możliwość konfiguracji parametru Max. Transmission Unit (MTU), Wsparcie dla protokołu SSDP, Obsługa protokołów TLS 1.2, SSL v3, Obsługa protokołu LDAP, Integracja z HP SIM, Synchronizacja czasu poprzez protokół NTP, Możliwość backupu i odtworzenia ustawień bios serwera oraz ustawień karty zarządzającej, Oprogramowanie zarządzające i diagnostyczne wyprodukowane przez producenta serwera umożliwiające konfigurację kontrolera RAID, instalację systemów operacyjnych, zdalne zarządzanie, diagnostykę i przewidywanie awarii w oparciu o informacje dostarczane w ramach zintegrowanego w serwerze systemu umożliwiającego monitoring systemu i środowiska (m.in. temperatura, dyski, zasilacze, płyta główna, procesory, pamięć operacyjna); Opcjonalna wbudowana w kartę zarządzającą (lub zainstalowana) pamięć flash o pojemności minimum 16 GB; Możliwość zdalnej reinstalacji systemu lub aplikacji z obrazów zainstalowanych w obrębie dedykowanej pamięci flash bez użytkowania zewnętrznych nośników lub kopiowania danych poprzez sieć LAN; Serwer posiada opcjonalną możliwość konfiguracji i wykonania aktualizacji BIOS, Firmware, sterowników serwera bezpośrednio z GUI (graficzny interfejs) karty zarządzającej serwera bez pośrednictwa innych nośników zewnętrznych i wewnętrznych poza obrębem karty zarządzającej. **Wspierane OS** Microsoft Windows Server 2019, 2016; VMWare vSphere 6.7; Suse Linux Enterprise Server 12; Red Hat Enterprise Linux 7; **Gwarancja** 5 lat gwarancji producenta serwera w trybie onsite z gwarantowanym przyjazdem do miejsca użytkowania sprzętu certyfikowanego przez producenta pracownika serwisu do końca następnego dnia roboczego; Zgłaszanie usterek i awarii sprzętowych poprzez automatyczne założenie zgłoszenia w systemie helpdesk/servicedesk producenta sprzętu (bez udziału administratora) – opcja rozbudowy; Firma serwisująca musi posiadać ISO 9001:2000 na świadczenie usług serwisowych; Bezpłatna dostępność poprawek i aktualizacji BIOS/Firmware/sterowników dożywotnio dla oferowanego serwera – jeżeli funkcjonalność ta wymaga dodatkowego serwisu lub licencji producenta serwera, takowy element musi być uwzględniona w ofercie; Możliwość odpłatnego wydłużenia gwarancji producenta do 7 lat w trybie onsite z gwarantowanym skutecznym zakończeniem naprawy serwera najpóźniej w następnym dniu roboczym od zgłoszenia usterki (podać koszt na dzień składania oferty); **Dokumentacja, inne** Elementy, z których zbudowane są serwery muszą być produktami producenta tych serwerów lub być przez niego certyfikowane oraz całe muszą być objęte gwarancją producenta, o wymaganym w specyfikacji poziomie SLA – wymaganie oświadczenie wykonawcy; Serwer musi być fabrycznie nowy i pochodzić z oficjalnego kanału dystrybucyjnego w UE – wymagane oświadczenie wykonawcy; Ogólnopolska, telefoniczna infolinia/linia techniczna producenta serwera, w ofercie należy podać link do strony producenta na której znajduje się nr telefonu oraz maila na który można zgłaszać usterki; W czasie obowiązywania gwarancji na sprzęt, możliwość po podaniu na infolinii numeru seryjnego urządzenia weryfikacji pierwotnej konfiguracji sprzętowej serwera, w tym model i typ dysków twardych, procesora, ilość fabrycznie zainstalowanej pamięci operacyjnej, czasu obowiązywania i typ udzielonej gwarancji; Możliwość aktualizacji i pobrania sterowników do oferowanego modelu serwera w najnowszych certyfikowanych wersjach bezpośrednio z sieci Internet za pośrednictwem strony www producenta serwera;

Serwerowy system operacyjny musi posiadać następujące, wbudowane cechy oraz zainstalowany na serwerze wraz z aktualizacjami.

1. Możliwość wykorzystania 320 logicznych procesorów oraz co najmniej 4 TB pamięci RAM w środowisku fizycznym.
2. Możliwość wykorzystywania 64 procesorów wirtualnych oraz 1TB pamięci RAM i dysku o pojemności do 64TB przez każdy wirtualny serwerowy system operacyjny.

3. Możliwość budowania klastrów składających się z 64 węzłów, z możliwością uruchamiania 7000 maszyn wirtualnych.
4. 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.
5. Wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany pamięci RAM bez przerywania pracy.
6. Wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany procesorów bez przerywania pracy.
7. Automatyczna weryfikacja cyfrowych sygnatur sterowników w celu sprawdzenia, czy sterownik przeszedł testy jakości przeprowadzone przez producenta systemu operacyjnego.
8. Możliwość dynamicznego obniżania poboru energii przez rdzenie procesorów niewykorzystywane w bieżącej pracy. Mechanizm ten musi uwzględniać specyfikę procesorów wyposażonych w mechanizmy Hyper-Threading.
9. Wbudowane wsparcie instalacji i pracy na wolumenach, które:
    a. pozwalają na zmianę rozmiaru w czasie pracy systemu,
    b. umożliwiają tworzenie w czasie pracy systemu migawek, dających użytkownikom końcowym (lokalnym i sieciowym) prosty wgląd w poprzednie wersje plików i folderów,
    c. umożliwiają kompresję "w locie" dla wybranych plików i/lub folderów,
    d. umożliwiają zdefiniowanie list kontroli dostępu (ACL).
10. Wbudowany mechanizm klasyfikowania i indeksowania plików (dokumentów) w oparciu o ich zawartość.
11. Wbudowane szyfrowanie dysków przy pomocy mechanizmów posiadających certyfikat FIPS 140-2 lub równoważny wydany przez NIST lub inną agendę rządową zajmującą się bezpieczeństwem informacji.
12. Możliwość uruchamianie aplikacji internetowych wykorzystujących technologię ASP.NET
13. Możliwość dystrybucji ruchu sieciowego HTTP pomiędzy kilka serwerów.
14. Wbudowana zapora internetowa (firewall) z obsługą definiowanych reguł dla ochrony połączeń internetowych i intranetowych.
15. Dostępne dwa rodzaje graficznego interfejsu użytkownika:
    a. Klasyczny, umożliwiający obsługę przy pomocy klawiatury i myszy,
    b. Dotykowy umożliwiający sterowanie dotykiem na monitorach dotykowych.
16. Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, przeglądarka internetowa, pomoc, komunikaty systemowe,
17. Możliwość zmiany języka interfejsu po zainstalowaniu systemu, dla co najmniej 10 języków poprzez wybór z listy dostępnych lokalizacji.
18. Mechanizmy logowania w oparciu o:
    a. Login i hasło,
    b. Karty z certyfikatami (smartcard),
    c. Wirtualne karty (logowanie w oparciu o certyfikat chroniony poprzez moduł TPM),
19. Możliwość wymuszania wieloelementowej dynamicznej kontroli dostępu dla: określonych grup użytkowników, zastosowanej klasyfikacji danych, centralnych polityk dostępu w sieci, centralnych polityk audytowych oraz narzuconych dla grup użytkowników praw do wykorzystywania szyfrowanych danych..

20. Wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug&Play).
21. Możliwość zdalnej konfiguracji, administrowania oraz aktualizowania systemu.
22. Dostępność bezpłatnych narzędzi producenta systemu umożliwiających badanie i wdrażanie zdefiniowanego zestawu polityk bezpieczeństwa.
23. Pochodzący od producenta systemu serwis zarządzania polityką dostępu do informacji w dokumentach (Digital Rights Management).
24. Wsparcie dla środowisk Java i .NET Framework 4.x – możliwość uruchomienia aplikacji działających we wskazanych środowiskach.
25. Możliwość implementacji następujących funkcjonalności bez potrzeby instalowania dodatkowych produktów (oprogramowania) innych producentów wymagających dodatkowych licencji:
    a. Podstawowe usługi sieciowe: DHCP oraz DNS wspierający DNSSEC,
    b. Usługi katalogowe oparte o LDAP i pozwalające na uwierzytelnianie użytkowników stacji roboczych, bez konieczności instalowania dodatkowego oprogramowania na tych stacjach, pozwalające na zarządzanie zasobami w sieci (użytkownicy, komputery, drukarki, udziały sieciowe), z możliwością wykorzystania następujących funkcji:
        - odłączenie do domeny w trybie offline – bez dostępnego połączenia sieciowego z domeną,
        - Ustanawianie praw dostępu do zasobów domeny na bazie sposobu logowania użytkownika – na przykład typu certyfikatu użytego do logowania,
        - Odzyskiwanie przypadkowo skasowanych obiektów usługi katalogowej z mechanizmu kosza.
        - Bezpieczny mechanizm dołączania do domeny uprawnionych użytkowników prywatnych urządzeń mobilnych opartych o iOS i Windows 8.1.
    c. Zdalna dystrybucja oprogramowania na stacje robocze.
    d. Praca zdalna na serwerze z wykorzystaniem terminala (cienkiego klienta) lub odpowiednio skonfigurowanej stacji roboczej
    e. Centrum Certyfikatów (CA), obsługa klucza publicznego i prywatnego) umożliwiające:
        - Dystrybucję certyfikatów poprzez http
        - Konsolidację CA dla wielu lasów domeny,
        - Automatyczne rejestrowania certyfikatów pomiędzy różnymi lasami domen,
        - Automatyczne występowanie i używanie (wystawianie) certyfikatów PKI X.509.
    f. Szyfrowanie plików i folderów.
    g. Szyfrowanie połączeń sieciowych pomiędzy serwerami oraz serwerami i stacjami roboczymi (IPSec).
    h. Możliwość tworzenia systemów wysokiej dostępności (klastry typu fail-over) oraz rozłożenia obciążenia serwerów.
    i. Serwis udostępniania stron WWW.
    j. Wsparcie dla protokołu IP w wersji 6 (IPv6),
    k. Wsparcie dla algorytmów Suite B (RFC 4869),

l. Wbudowane usługi VPN pozwalające na zestawienie nielimitowanej liczby równoczesnych połączeń i niewymagające instalacji dodatkowego oprogramowania na komputerach z systemem Windows,
m. Wbudowane mechanizmy wirtualizacji (Hypervisor) pozwalające na uruchamianie do 1000 aktywnych środowisk wirtualnych systemów operacyjnych. Wirtualne maszyny w trakcie pracy i bez zauważalnego zmniejszenia ich dostępności mogą być przenoszone pomiędzy serwerami klastra typu failover z jednoczesnym zachowaniem pozostałej funkcjonalności. Mechanizmy wirtualizacji mają zapewnić wsparcie dla:

- Dynamicznego podłączania zasobów dyskowych typu hot-plug do maszyn wirtualnych,
- Obsługi ramek typu jumbo frames dla maszyn wirtualnych.
- Obsługi 4-KB sektorów dysków
- Nielimitowanej liczby jednocześnie przenoszonych maszyn wirtualnych pomiędzy węzłami klastra
- Możliwości wirtualizacji sieci z zastosowaniem przełącznika, którego funkcjonalność może być rozszerzana jednocześnie poprzez oprogramowanie kilku innych dostawców poprzez otwarty interfejs API.
- Możliwości kierowania ruchu sieciowego z wielu sieci VLAN bezpośrednio do pojedynczej karty sieciowej maszyny wirtualnej (tzw. trunk mode)

26. Możliwość automatycznej aktualizacji w oparciu o poprawki publikowane przez producenta wraz z dostępnością bezpłatnego rozwiązania producenta serwerowego systemu operacyjnego umożliwiającego lokalną dystrybucję poprawek zatwierdzonych przez administratora, bez połączenia z siecią Internet.
27. Wsparcie dostępu do zasobu dyskowego poprzez wiele ścieżek (Multipath).
28. Możliwość instalacji poprawek poprzez wgranie ich do obrazu instalacyjnego.
29. Mechanizmy zdalnej administracji oraz mechanizmy (również działające zdalnie) administracji przez skrypty.
30. Możliwość zarządzania przez wbudowane mechanizmy zgodne ze standardami WBEM oraz WS-Management organizacji DMTF.
31. Zorganizowany system szkoleń i materiały edukacyjne w języku polskim.

5. Stacje robocze z monitorem, z system operacyjnym oraz z pakietem biurowym - szt. 10

Specyfikacja procesora-minimalne parametry: Liczba rdzeni 6, Liczba wątków 12, Maks. częstotliwość turbo 4.40 GHz, Maksymalna częstotliwość turbo rdzeni Performance-core 4.40 GHz, Częstotliwość bazowa rdzeni Performance-core 2.50 GHz, Cache 18 MB Intel® Smart Cache, Łącznie pamięci podręcznej L2 7.5 MB, Liczba rdzeni procesora Min. 6, Maksymalne taktowanie procesora Min. 4,4 GHz, Cache procesora Min. 18 MB, Liczba procesorów 1; **Pamięć minimalne parametry**-Pamięć wewnętrzna Minimum 8 GB, Maksymalna pojemność pamięci Minimum 64 GB, Typ pamięci wewnętrznej DDR4-SDRAM, Układ pamięci 1 x 8 GB Gniazda pamięci Minimum DIMM x 2, Prędkość zegara pamięci Minimum 3200 Mhz; **Nośnik danych minimalne parametry**-Całkowita pojemność przechowywania Minimum 256 GB, Nośniki SSD, Napęd optyczny DVD±RW, Liczba zainstalowanych

dysków 1 Całkowita pojemność dysków SSD Minimum 256 GB Liczba zainstalowanych dysków SSD 1, Pojemność pamięci SSD Minimum 256 GB, NVMe Tak Rozmiar kieszeni dysku SSD M.2, **Grafika minimalne parametry** - Wbudowana karta graficzna Tak, Model wbudowanej karty graficznej Minimum Graphics 730; **Sieć porty minimum** Przewodowa sieć LAN Tak Prędkość transferu danych przez Ethernet LAN10/100/1000, Technologia okablowania 10/100/1000Base-T(X), Wi-Fi Nie; **Porty i interfejsy minimium** Liczba portów USB 2.0-4, Ilość portów USB 3.2 Gen 1 (3.1 Gen 1) Typu-A- 4, Ilość portów HDMI-1, Ilość DisplayPort 1,Wersja DisplayPort 1.4,Ilość portów Ethernet LAN (RJ-45) 1, Wyjście liniowe Tak, Port dla zestaw słuchawka/mikrofon Tak, **Konstrukcja-** Obudowa SFF, Kolor produktu Czarny; **Moc** Zasilanie - Max. 180 W Rozmiary Max. Szerokość produktu 92,7 mm, Głębokość produktu 292,9 mm, Wysokość produktu 291 mm

System operacyjny zainstalowany na komputerze– System 64 bitowy (z dostępną wersją 32-bitową), system operacyjny powinien być zainstalowany na komputerze wraz z oprogramowaniem oraz sterownikami urządzeń i składników wyposażenia komputera; gotowy do użytkowania; wszystkie niezbędne poprawki zalecane przez producenta systemu operacyjnego powinny być zainstalowane,

– Musi pozwalać na instalację oprogramowania użytkowanego na komputerach Urzędu w tym MS Office 2003, 2007,2010, 2016, 2019, 2021 w wersjach standard lub pro (w tym MS Access, Visio), programów firmy Adobe, Corel, Płatnik,

– Musi pozwalać na instalację i poprawne funkcjonowanie oprogramowania służącego do użytkowania podpisu kwalifikowanego KIR,

Licencja musi:

– Być nieograniczona w czasie,

– Pozwalać na instalację zarówno 64- jak i 32-bitowej wersji systemu

– Pozwalać na instalację na oferowanym sprzęcie nieograniczoną ilość razy bez konieczności kontaktowania się z producentem systemu lub sprzętu,

– Powinna mieć możliwość skonfigurowania przez administratora regularnego i automatycznego pobierania ze strony internetowej producenta systemu operacyjnego i instalowania aktualizacji i poprawek do systemu operacyjnego,

– Darmowe aktualizacje w ramach wersji systemu operacyjnego przez Internet (niezbędne aktualizacje, poprawki, biuletyny bezpieczeństwa muszą być dostarczane bez dodatkowych opłat); internetowa aktualizacja zapewniona w języku polskim,

– Na stronie WWW producenta komputera powinny być dostępne aktualne wersje kompletu sterowników do urządzeń i składników stanowiących wyposażenie dostarczanego komputera dla dostarczonego systemu operacyjnego.

– Musi mieć możliwość tworzenia wielu kont użytkowników o różnych poziomach uprawnień, zabezpieczonych hasłem dostęp do systemu, konta i profile użytkowników z opcją zarządzania zdalnego; praca systemu w trybie ochrony kont użytkowników,

– Musi mieć zintegrowaną zaporę sieciową oraz zintegrowaną z systemem konsolę do zarządzania ustawieniami zapory i regułami IP v4 i v6

– Musi być wyposażony w graficzny interfejs użytkownika w języku polskim

– Musi posiadać wbudowane co najmniej następujące elementy zlokalizowane w języku polskim: menu, system pomocy, komunikaty systemowe;

– Zdalna pomoc i współdzielenie aplikacji możliwość zdalnego przejęcia sesji zalogowanego użytkownika celem rozwiązania problemu z komputerem,

– Zintegrowane oprogramowanie do tworzenia kopii zapasowych (Backup systemu); automatyczne wykonywanie kopii plików z możliwością automatycznego przywrócenia wersji wcześniejszej; możliwość przywracania plików systemowych,

– Zintegrowany z systemem moduł wyszukiwania informacji o lokalizacji katalogów i plików różnego typu dostępny z kilku poziomów: poziom menu, poziom otwartego okna systemu operacyjnego,
– Musi być w pełni kompatybilny z oferowanym sprzętem - tj. zapewniać obsługę wszystkich wbudowanych urządzeń i zapewniać pełną funkcjonalność oferowanego sprzętu,
– Być zgodny z użytkowanym przez urzędu pakietem oprogramowana antywirusowego Eset Endpoint Security,
– Musi zapewniać wsparcie dla użytkowanych przez Urzędu oraz większości powszechnie używanych urządzeń i standardów dotyczących drukarek, skanerów, urządzeń sieciowych, USB, e-Sata, FireWare, Bluetooth, oraz urządzeń i nośników w trybie Plug & Play, WiFi,
– Nie może ograniczać możliwości instalacji w przyszłości nowego powszechnie dostępnego sprzętu (sterowniki) oraz oprogramowania,
W przypadku dostawy i zainstalowania przez Dostawcę systemu równoważnego zobowiązany jest on do pokrycia wszelkich kosztów wymaganych w czasie wdrożenia oferowanego rozwiązania, w szczególności z dostosowaniem infrastruktury informatycznej, oprogramowania nią zarządzającego, systemowego i narzędziowego, zapewnienia serwisu gwarancyjnego i pogwarancyjnego, szkoleń użytkowników sprzętu oraz szkoleń certyfikowanych dla administratorów systemów informatycznych i użytkowników w jednostce do której dostarczono oferowane rozwiązanie.
Do każdego komputera muszą być dołączone:
– płyta odtworzeniowa lub partycja na dysku twardym z systemem recovery pozwalająca przywrócić pełny stan fabryczny konfiguracji systemu operacyjnego i oprogramowania

Monitor

WYŚWIETLACZ -Przekątna ekranu Minimum 23.80 cali, Typ matrycy VA, Technologia podświetlania WLED, Format obrazu 16:9, Wielkość plamki 0.2750 mm, Czas reakcji matrycy Max. 4.0 ms, Jasność matrycy Minimum 250 cd/m2, Kontrast statyczny Minimum 3000 :1, Rozdzielczość Minimum 1920 x 1080 (Full HD), Częst. odświeżania przy rozdzielczości optymalnej Minimum 75 Hz, Częstotliwość odchylania pionowego 48-76 Hz, Częstotliwość odchylania poziomego 30-85 kHz, Ilość wyświetlanych kolorów 16,7 M (8-bitowy), Kąt widzenia pionowy (V) Minimum 178.00 stopni, Kąt widzenia poziomy (H) Minimum 178.00 stopni, Regulacja kąta nachylenia (Tilt) -5° / +20,TECHNICZNE Zgodność z technologią HDCP Tak, Redukcja migotania Tak, Wbudowane głośniki 2 x 2W, Montaż VESA 100 x 100, Wbudowany zasilacz Tak, ZŁĄCZA Złącza zewn. Minimum D-Sub / VGA; HDMI;Wyjście audio; ZUŻYCIE ENERGII-Pobór energii (podczas pracy) 14.37 W, Pobór energii (tryb czuwania) 0.50 W, Klasa energetyczna E; Kolor obudowy Czarny (Black); POZOSTAŁE PARAMETRY - Wyposażenie dodatkowe Przewód HDMI, przewód zasilający, Dokumentacja użytkownika
Zaoferowany komputer musi być wyposażony w zainstalowany pakiet biurowy
Oferowany pakiet biurowy musi spełniać minimalnie poniższe wymagania: • Wersja językowa: Pełna polska wersja językowa interfejsu użytkownika, • Oprogramowanie musi umożliwiać dostosowanie dokumentów i szablonów do potrzeb instytucji oraz udostępniać narzędzia umożliwiające dystrybucję odpowiednich szablonów do właściwych odbiorców, • W skład oprogramowania muszą wchodzić narzędzia programistyczne umożliwiające automatyzację pracy i wymianę danych pomiędzy dokumentami i aplikacjami (język makropoleceń, język skryptowy), • Do aplikacji musi być dostępna pełna dokumentacja w języku polskim, • Pakiet zintegrowanych aplikacji biurowych musi zawierać: – edytor tekstu wspierający formaty .docx – arkusz kalkulacyjny wspierający formaty .xlsx – narzędzie do przygotowywania i prowadzenia prezentacji wspierający formaty .pptx – narzędzie do tworzenia drukowanych materiałów informacyjnych, – narzędzie zarządzania informacją prywatą (pocztą elektroniczną, kalendarzem, kontaktami i zadaniami),

Minimalna wymagana funkcjonalność dotycząca edytora tekstu: • edycja 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, • sprawdzanie pisowni w języku polskim, • śledzenie zmian wprowadzonych przez użytkowników, • nagrywanie, tworzenie i edycję makr automatyzujących wykonywanie czynności, • określenie układu strony (pionowa/pozioma), • 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.
Minimalna wymagana funkcjonalność dotycząca arkusza kalkulacyjnego: • tworzenie raportów tabelarycznych, • tworzenie wykresów liniowych (wraz z 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 zmianę 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 polskich formatem, • zapis wielu arkuszy kalkulacyjnych w jednym pliku, • zabezpieczenie dokumentów hasłem przed odczytem, oraz przed wprowadzaniem modyfikacji.
Minimalna wymagana funkcjonalność dotycząca narzędzia do przygotowania i prowadzenia prezentacji: • przygotowanie prezentacji multimedialnych, które będą prezentowane 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 tabeli 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.
Minimalna wymagana funkcjonalność dotycząca narzędzia do tworzenia drukowanych materiałów informacyjnych: • tworzenie i edycję drukowanych materiałów informacyjnych, • tworzenie materiałów przy użyciu dostępnych z narzędziem szablonów: broszur, biuletynów, katalogów, • edycję poszczególnych stron materiałów, • podział treści na kolumny, • umieszczanie elementów graficznych, • wykorzystanie mechanizmu korespondencji seryjnej, • płynne przesuwanie elementów po całej stronie publikacji, • eksport publikacji do formatu PDF oraz TIFF, • wydruk publikacji, • możliwość przygotowania materiałów do wydruku w standardzie CMYK.
Minimalna wymagana funkcjonalność dotycząca narzędzia do zarządzania informacją prywatną (pocztą elektroniczną, kalendarzem, kontaktami i zadaniami): • pobieranie i

wysyłanie poczty elektronicznej z serwera pocztowego, • 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, • zarządzanie kalendarzem, • udostępnianie kalendarza innym użytkownikom, • przeglądanie kalendarza innych użytkowników, • zaproszenie 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 użytkownikom. Licencja wieczysta.

Okres gwarancji w miesiącach minimum: 36 miesięcy
Czas naprawy to następny dzień roboczy
Naprawy realizowane na miejscu w siedzibie Klienta

6. **Zakup oprogramowania do monitorowania sieci i użytkowników, inwentaryzacji sprzętu i oprogramowania, zdalnej pomocy technicznej oraz ochrony danych przed wyciekiem i zainfekowaniem dla 25 użytkowników;**

Wymagane funkcje:

- minimalizacja zjawiska cyberslackingu i zwiększenie wydajności pracowników
- redukcja kosztów wydruku
- blokowanie stron WWW
- blokowanie uruchamianych aplikacji
- monitorowanie wiadomości e-mail (nagłówki) - antyphishing
- szczegółowy czas pracy (godzina rozpoczęcia i zakończenia aktywności oraz przerwy)
- użytkowane aplikacje (aktywnie i nieaktywnie)
- odwiedzane strony WWW (tytuły i adresy stron, liczba i czas wizyt)
- audyty wydruków (drukarka, użytkownik, komputer), koszty wydruków
- użycie łącza: generowany przez użytkowników ruch sieciowy
- statyczny zdalny podgląd pulpitu użytkownika (bez dostępu)
- zrzuty ekranowe (historia pracy użytkownika ekran po ekranie)
- blokowanie uruchamiania procesów na podstawie lokalizacji pliku .EXE
- zarządzanie regułami blokowania aplikacji i stron WWW (tworzenie, grupowanie, powielanie między grupami użytkowników)
- skanowanie sieci, wykrywanie urządzeń i serwisów TCP/IP
- interaktywne mapy sieci, mapy użytkownika, oddziałów, mapy inteligentne
- jednoczesna praca wielu administratorów, zarządzanie uprawnieniami, dzienniki dostępu
- serwisy TCP/IP: poprawność i czas odpowiedzi, statystyka ilości odebranych/utraconych pakietów (PING, SMB, HTTP, POP3, SNMP, IMAP, SQL itp.)
- liczniki WMI: obciążenie procesora, zajętość pamięci, zajętość dysków, transfer sieciowy itp.
- możliwość nakładania na urządzenie liczników wydajności wg szablonu (wzorca)

- działanie Windows: zmiana stanu usług (uruchomienie, zatrzymanie, restart), wpisy dziennika zdarzeń
- liczniki SNMP v1/2/3 (np. transfer sieciowy, temperatura, wilgotność, napięcie zasilania, poziom tonera i inne)
- kompilator plików MIB
- obsługa pułapek SNMP
- routery i switche: mapowanie portów
- obsługa komunikatów syslog
- alarmy zdarzenie - akcja
- powiadomienia (pulpitowe, e-mail, SMS) oraz akcje korekcyjne (uruchomienie programu, restart komputera itp.)
- raporty (dla urządzenia, oddziału, wybranej mapy lub całej sieci)
- audyt inwentaryzacji sprzętu i oprogramowania
- wgląd w licencje przypisane do użytkownika pracującego na wielu urządzeniach
- zdalny dostęp do managera plików z możliwością usuwania plików użytkownika
- informacje o wpisach rejestrowych, plikach i archiwach .zip na stacji roboczej
- szczegółowe informacje o konfiguracji sprzętowej konkretnej stacji roboczej
- zarządzanie instalacjami/dezinstalacjami oprogramowania w oparciu o menedżera pakietów MSI
- alarmy: instalacja oprogramowania, zmiana w zasobach sprzętowych
- lista kluczy oprogramowania Microsoft
- aplikacja dla systemu Android umożliwiająca spis z natury na bazie kodów kreskowych, kodów QR
- możliwość archiwizacji i porównywania audytów
- monitorowanie harmonogramu zadań Windows
- dokumenty prawne dot. ochrony sygnalistów w tym szablon regulaminu zgłoszeń wewnętrznych wymagany przez Dyrektywę
- dwa tryby widoku - jasny i ciemny
- planowanie zastępstw w przydzielaniu zgłoszeń
- rozbudowany system raportów
- powiadomienia i widok zgłoszenia odświeżany w czasie rzeczywistym
- baza zgłoszeń z rozbudowaną wyszukiwarką
- baza wiedzy z kategoryzacją artykułów i możliwością wstawiania grafik oraz filmów z YouTube
- przejrzysty i intuicyjny interfejs webowy
- wewnętrzny komunikator (czat) z możliwością przydzielania uprawnień oraz przesyłania plików i tworzenia rozmów grupowych
- komunikaty wysyłane do użytkowników/komputerów z możliwym/obowiązkowym potwierdzeniem odczytu
- zdalny dostęp do komputerów z możliwością blokady myszy/klawiatury
- dwukierunkowa wymiana plików
- zarządzanie procesami Windows z poziomu okna informacji o urządzeniu
- zadania dystrybucji oraz uruchamiania plików (zdalna instalacja oprogramowania)
- procesowanie zgłoszeń z wiadomości e-mail
- integracja bazy użytkowników z Active Directory
- zarządzanie kontami lokalnych użytkowników Windows (tworzenie, usuwanie, edycja, reset hasła, eskalacja/deeskalacja uprawnień oraz włączanie/wyłączanie kont)
- zdalna edycja rejestru na komputerach z zainstalowanym agentem
- zdefiniowanie polityki przenoszenia danych firmowych przez pracowników wraz z odpowiednimi uprawnieniami

- informacje o urządzeniach podłączonych do danego komputera
- lista wszystkich urządzeń podłączonych do komputerów w sieci
- audyt (historia) podłączeń i operacji na urządzeniach przenośnych oraz na udziałach sieciowych
- zarządzanie prawami dostępu (zapis, uruchomienie, odczyt) dla urządzeń, komputerów i użytkowników
- centralna konfiguracja: ustawienie reguł dla całej sieci, dla wybranych map sieci oraz dla grup i użytkowników Active Directory
- integracja bazy użytkowników i grup z Active Directory
- alarmy: podłączono/odłączono urządzenie mobilne, operacja na plikach na urządzeniu mobilnym
- licencja na czas nieoznaczony.

II. ***Wymagany termin realizacji do 15.11.2022***

III. **Kryteria oceny ofert i ich wagi:**

1. Ocenie według poniższych kryteriów będą podlegać tylko oferty nieodrzucone oraz spełniające wszystkie wymogi formalne określone w ogłoszeniu.
2. Ocena ofert zostanie przeprowadzona wyłącznie w oparciu o przedstawione poniżej kryterium:
   Cena brutto za całość zamówienia – 100%.

IV. Oferty należy składać w terminie do **14 października 2022 r.** w sekretariacie Urzędu Gminy i Miasta Mogielnica ul. Rynek 1 do godziny **10:00.** W zaklejonej kopercie z napisem „Cyfrowa Gmina Zakup i Dostawa sprzętu komputerowego i oprogramowania"

Na załączonym formularzy oferty.

V.

BURMISTRZ
dr Sławomir Chmielewski

Załączniki:
1. Formularz oferty
2. Istotne postanowienia umowy

Przygotował:
Tomasz Kowalski
Tel. 486635149 w.25
gmina@mogielnica.pl