**Załącznik nr 7 do SWZ**

**OPIS PRZEDMIOTU ZAMÓWIENIA**

Dostawa sprzętu komputerowego oraz wdrożenie systemów i rozwiązań teleinformatycznych

w ramach Programu Operacyjnego Polska Cyfrowa na lata 2014-2020 Osi Priorytetowej V Rozwój cyfrowy JST oraz wzmocnienie cyfrowej odporności na zagrożenia REACT-EU

 działania 5.1 Rozwój cyfrowy JST oraz wzmocnienie cyfrowej odporności na zagrożenia

dotycząca realizacji projektu grantowego

**„Cyfrowa Gmina”** o numerze **POPC.05.01.00-00-0001/21-00**

Opis przedmiotu zamówienia wg Wspólnego Słownika Zamówień (CPV):

30200000-1 Urządzenia komputerowe

30213000-5 Komputery osobiste

48620000-0 Systemy operacyjne

48000000-8 Pakiety oprogramowania i systemy informatyczne

48820000-2 Serwery

51610000-1 Usługi instalowania urządzeń komputerowych i przetwarzania informacji

72265000-0 Usługi konfiguracji oprogramowania

Zawartość:

1. Ogólny opis przedmiotu zamówienia i wymagań Zamawiającego
2. Szczegółowe właściwości i wymagania funkcjonalno-użytkowe
3. Sprzęt komputerowy oraz urządzenie peryferyjne
4. Oprogramowanie biurowe i antywirusowe
5. System składowania i archiwizacji danych oraz wykonywania kopii zapasowych
6. Usługi wdrożeniowe w zakresie konfiguracji urządzeń sieci LAN oraz Firewall
7. Warunki uruchomienia i odbioru wdrożonych rozwiązań oraz przekazania do eksploatacji

1. **OGÓLNY OPIS PRZEDMIOTU ZAMÓWIENIA I WYMAGAŃ**

**ZAMAWIAJĄCEGO**

1. **Zakres przedmiotu zamówienia**

Przedmiotem zamówienia jest dostawa sprzętu komputerowego oraz wdrożenie systemów i rozwiązań teleinformatycznych mających na celu podniesienie poziomu cyfryzacji Jednostki w ramach Programu Operacyjnego Polska Cyfrowa na lata 2014-2020 Osi Priorytetowej V Rozwój cyfrowy JST oraz wzmocnienie cyfrowej odporności na zagrożenia REACT-EU działania 5.1 Rozwój cyfrowy JST oraz wzmocnienie cyfrowej odporności na zagrożenia dotycząca realizacji projektu grantowego **„Cyfrowa Gmina”** o numerze **POPC.05.01.00-00-0001/21-00**

Szczegółowy zakres projektu składa się z następujących zadań:

1. Dostawa sprzętu komputerowego oraz urządzenia peryferyjnego
* Stacje robocze – 18 kpl.
* Laptop – 1 szt.
* Urządzenie wielofunkcyjne A3 kolor - 1 szt.
1. Oprogramowanie biurowe i antywirusowe
* Oprogramowanie biurowe dla stacji roboczych – 19 lic.
* Oprogramowanie antywirusowe dla stacji roboczych - 19 lic.
1. Dostawa i instalacja oraz konfiguracja systemu składowania i archiwizacji danych oraz wykonywania kopii zapasowych
	* + Serwer NAS Tower – 1 szt.
		+ Dysk 2,5" 480 GB SSD – 2 szt.
2. Usługi wdrożeniowe w zakresie konfiguracji urządzeń sieci LAN oraz Firewall
* Usługi rekonfiguracji sieci LAN (przełączniki, router) – 1 kpl.
* Usługi rekonfiguracji Firewall – 1 kpl.
1. **Ogólne wymagania Zamawiającego**

 Niniejszy dokument ma celu umożliwienie dokonania wyboru najkorzystniejszej oferty na dostawy i usługi teleinformatyczne, których podstawowym celem jest podniesienie poziomu cyfryzacji Urzędu oraz bezpieczeństwa teleinformatycznego (cyberbezpieczeństwa). Dokument zawiera opis wymagań pod kątem kryteriów funkcjonalnych, technicznych i jakościowych, oraz wskazuje technologie, które powinny być wykorzystane tak aby osiągnąć założone cele i zapewnić optymalną relację ceny do jakości rozwiązania.

Opisane w dokumencie wymagania należy traktować jako podstawowe i minimalne.

W przypadkach, kiedy w opisie przedmiotu zamówienia wskazane zostały znaki towarowe, patenty, pochodzenie, źródło lub szczególny proces, który charakteryzuje produkty lub usługi dostarczane przez konkretnego wykonawcę co prowadziłoby do uprzywilejowania lub wyeliminowania niektórych wykonawców lub produktów, oznacza to, że Zamawiający nie może opisać przedmiotu zamówienia za pomocą dostatecznie dokładnych określeń i jest to uzasadnione specyfiką przedmiotu zamówienia. W takich sytuacjach ewentualne wskazania na znaki towarowe, patenty, pochodzenie, źródło lub szczególny proces, należy odczytywać z wyrazami „lub równoważne”

W sytuacjach, kiedy Zamawiający opisuje przedmiot zamówienia poprzez odniesienie się do norm, europejskich ocen technicznych, aprobat, specyfikacji technicznych i systemów referencji technicznych, o których mowa w art. 101 ust. 1 pkt 2 i ust. 3 ustawy Pzp, Zamawiający dopuszcza rozwiązania równoważne, a wskazane powyżej odniesienia należy odczytywać z wyrazami „lub równoważne”.

W przypadku zastosowania materiałów, urządzeń, wyrobów lub rozwiązań równoważnych, Wykonawca zobowiązany jest do ich wskazania w ofercie oraz do złożenia wraz z ofertą kart technicznych lub innych dokumentów potwierdzających, że oferowane rozwiązania równoważne spełniają wymagania Zamawiającego opisane w przedmiocie zamówienia.

**Wymagania ogólne dotyczące sprzętu:**

1. Wszystkie dostarczone urządzenia muszą być fabrycznie nowe, bez wad i uszkodzeń, nieregenerowane, nieużywane i nie będące przedmiotem wystaw i prezentacji oraz o ile nie wyspecyfikowano inaczej w wymaganiach szczegółowych dla urządzeń, wyprodukowane nie wcześniej **niż w 2021 roku.**
2. Wszystkie urządzenia będą pochodziły z oficjalnego, europejskiego kanału dystrybucji.
3. Urządzenia zostaną dostarczone przez Wykonawcę własnym transportem i na własny koszt w miejsce wskazane przez Zamawiającego. Wszystkie urządzenia muszą być dostarczone w oryginalnych opakowaniach producenta,
4. Wszystkie urządzenia powinny być zgodne z normami UE i przeznaczone na rynek UE, oraz powinny posiadać certyfikat CE.
5. Dostarczany sprzęt powinien być kompletny i gotowy do uruchomienia, tak aby nie był konieczny zakup dodatkowych elementów czy akcesoriów,
6. Wykonawca dostarczy stosowne potwierdzenie gwarancji sprzętu i oprogramowania zapewniające, że sprzęt objęty jest gwarancją producenta
7. Serwis sprzętu będzie świadczony przez producenta lub jego autoryzowanego partnera serwisowego posiadającego wdrożoną normę min. PN-EN ISO 9001 lub równoważną.
8. Sprzęt dostarczany w ramach niniejszego zamówienia, powinien być objęty 36 miesięczną gwarancją i wsparciem producenta chyba, że okres i warunki gwarancji zostały dodatkowo określony w opisie szczegółowym specyfikowanego wyposażenia/sprzętu. W okresie gwarancji Wykonawca jest zobowiązany zapewnić Zamawiającemu:
	1. usuwanie wszelkich wad i nieprawidłowości powstałych na wskutek standardowej i zgodnej z przeznaczeniem eksploatacji przedmiotu zamówienia,
	2. przyjmowanie zgłoszeń serwisowych w godzinach 8.00-20.00 (faks lub e-mail) z możliwością zgłaszania awarii bezpośrednio u producenta (na wypadek braku reakcji serwisowej ze strony Wykonawcy),
	3. dostęp do bezpośredniego wsparcia technicznego producenta wraz z prawem do aktualizacji oprogramowania systemowego.
9. W ramach gwarancji wymagane jest wsparcie producenta sprzętu, a czas reakcji na zgłoszenia będzie realizowany w trybie następny dzień roboczy w miejscu instalacji i zastrzeżeniem, że uszkodzone nośniki danych pozostają u Zamawiającego. Ponadto wymagane jest, aby dostarczony poziom wsparcia producenta dawał możliwość kategoryzacji zgłoszeń i w przypadku awarii krytycznych gwarantował natychmiastową pomoc telefoniczną, szybką interwencję specjalisty ds. eskalacji zgłoszeń oraz wizytę serwisanta i/lub wysyłkę uszkodzonych części
10. Udzielona gwarancja producenta nie wyłącza uprawnień Zamawiającego z tytułu rękojmi w stosunku do Wykonawcy.

**Wymagania ogólne dotyczące oprogramowania:**

Wykonawca zobowiązany jest dostarczyć Zamawiającemu:

1. certyfikaty licencyjne wystawione przez producenta Oprogramowania, o ile nie są dostępne w formie elektronicznej na dedykowanym portalu klienckim;
2. nośniki instalacyjne Oprogramowania, o ile nie są dostępne w formie elektronicznej na dedykowanym portalu klienckim;
3. adresy poczty elektronicznej, numery telefonów oraz inne dane dostępowe umożliwiające Zamawiającemu korzystanie ze Wsparcia technicznego świadczonego przez producenta Oprogramowania w pełnym zakresie, o ile nie są dostępne w formie elektronicznej na ogólnodostępnym lub dedykowanym portalu klienckim;
4. zestawienie dostarczonych Zamawiającemu pozycji w zakresie Oprogramowania, zawierające m.in.: numer partii (SKU), pełna nazwa produktu, wersja i edycja oprogramowania, metryka licencyjna, rodzaj licencji (terminowa/bezterminowa), okres obowiązywania licencji, okres obowiązywania wsparcia technicznego, poziom wsparcia technicznego,
5. standardowe warunki licencyjne producenta Oprogramowania, o ile nie są dostępne w formie elektronicznej na ogólnodostępnym lub dedykowanym portalu klienckim;
6. standardowe warunki Wsparcia technicznego producenta Oprogramowania, o ile nie są dostępne w formie elektronicznej na ogólnodostępnym lub dedykowanym portalu klienckim;
7. oświadczenie producenta Oprogramowania potwierdzające dostawę licencji i objęcie ich wsparciem technicznym na poziomie zgodnym z wymaganiami Zamawiającego, o ile nie potwierdzają jej certyfikaty licencyjne i standardowe warunki Wsparcia technicznego;

Realizacja powyższego zakresu zamówienia musi być wykonana w oparciu o obowiązujące przepisy, przez Wykonawcę posiadającego stosowne doświadczenie, uprawnienia i potencjał wykonawczy oraz osoby o odpowiednich kwalifikacjach i doświadczeniu zawodowym.

1. **SZCZEGÓŁOWE WŁAŚCIWOŚCI I WYMAGANIA FUNKCJONALNO - UŻYTKOWE**
2. **Dostawa sprzętu komputerowego oraz urządzenia peryferyjnego**
	1. **Stacje robocze (komputer AiO) - 18 kpl.**

|  |  |
| --- | --- |
| **Parametr lub warunek**  | **Minimalne wymagania**  |
| Typ | Komputer stacjonarny. Typu All in One, komputer fabrycznie wbudowany w obudowę monitora. **W ofercie wymagane jest podanie modelu producenta komputera.** |
| Zastosowanie | Komputer będzie wykorzystywany dla potrzeb aplikacji biurowych, aplikacji edukacyjnych, aplikacji obliczeniowych, dostępu do Internetu oraz poczty elektronicznej, jako lokalna baza danych, stacja programistyczna |
| Wydajność | Procesor wielordzeniowy zaprojektowany do pracy w komputerach stacjonarnych klasy x86.Procesor 64 bitowy o architekturze x86, o wydajności min. 10000 pkt w teście CPU Mark zgodnie z https://www.cpubenchmark.net/cpu\_list.php**Wykonawca w składanej ofercie winien podać dokładny model oferowanego podzespołu.** |
| Pamięć operacyjna | 8GB możliwość rozbudowy do 64GB, jeden slot wolny |
| Pamięć masowa | **500GB SSD M.2 NVMe**Możliwość instalacji dodatkowego dysku twardego |
| Grafika | Grafika zintegrowana z procesorem powinna umożliwiać pracę min. dwumonitorową, współdzielona i dynamicznie przydzielana pamięć z RAM,  |
| Ekran | **Rozmiar matrycy / plamki min. 23,8” / max. 0,275mm** Rozdzielczość FHD (1920x1080)Jasność typowa min. 250 cd/m² Kontrast typowy 1000:1Barwa koloru (typowa) 72% NTSCKąty typowe 178(+/- 89) / 178 (+/-89)Rodzaj matrycy Matowa IPS |
| Multimedia | Karta dźwiękowa zintegrowana z płytą główną, wbudowane dwa głośniki min. 2W na kanał. Wbudowana w obudowę matrycy cyfrowa kamera 2,0 MP. Mechanicznie chowana w obudowie ( nie dopuszcza się kamer przekręcanych i wystających poza obrys obudowy)Wbudowane w obudowę dwa mikrofony  |
| Obudowa | Typu All-in-One zintegrowana z monitorem min. 24”. Obudowa musi umożliwiać zastosowanie zabezpieczenia fizycznego w postaci linki metalowej lub kłódki (oczko w obudowie do założenia kłódki), Demontaż tylnej pokrywy musi odbywać się bez użycia narzędzi. Komputer musi posiadać możliwość zainstalowania na ścianie przy wykorzystaniu ściennego systemu montażowego VESA 100,Zasilacz wewnętrzny o mocy min. 155W o efektywności min. 85% przy obciążeniu zasilacza na poziomie 50% oraz o efektywności min. 82% przy obciążeniu zasilacza na poziomie 100%, Zasilacz w oferowanym komputerze musi się znajdować na stronie <http://www.plugloadsolutions.com/80pluspowersupplies.aspx>, do oferty należy dołączyć wydruk potwierdzający spełnienie wymogu 80plusWbudowany w obudowie wizualny system diagnostyczny, służący do sygnalizowania i diagnozowania problemów z komputerem i jego komponentami, w szczególności: uszkodzenia lub braku pamięci RAM, uszkodzenia płyty głównej, awarii procesora. System musi zapisywać logi zdarzeń w BIOS. System diagnostyczny nie może wykorzystywać minimalnej ilości wolnych slotów wymaganych w specyfikacji. Każdy komputer musi być oznaczony niepowtarzalnym numerem seryjnym umieszonym na obudowie oraz wpisanym na stałe w BIOS.Podstawa jednostki typu All – in – One musi umożliwiać:Regulację pochyłu pionowego w zakresie od -5 do 30 stopni.Regulację wysokości w zakresie minimum 10 cm.Ustawienie jednostki w trybie Pivot.Obrót podstawy w lewą oraz prawą stronę. |
| Zgodność z systemami operacyjnymi i standardami | Oferowane modele komputerów muszą poprawnie współpracować z zamawianymi systemami operacyjnymi (jako potwierdzenie poprawnej współpracy Wykonawca dołączy do oferty dokument w postaci wydruku potwierdzający certyfikację rodziny produktów bez względu na rodzaj obudowy, dodatkowo potwierdzony przez producenta oferowanego komputera). |
| Zarządzanie | Wbudowana w płytę główną technologia zarządzania i monitorowania komputerem na poziomie sprzętowym działająca niezależnie od stanu czy obecności systemu operacyjnego oraz stanu włączenia komputera podczas pracy na zasilaczu sieciowym AC, obsługująca zdalną komunikację sieciową w oparciu o protokół IPv4 oraz IPv6, a także zapewniająca min.:-Monitorowanie konfiguracji komponentów komputera - CPU, Pamięć, HDD wersja BIOS płyty głównej; -Zdalną konfigurację ustawień BIOS,-Zdalne przejęcie konsoli tekstowej systemu, przekierowanie procesu ładowania systemu operacyjnego z wirtualnego CD ROM lub FDD z serwera zarządzającego;-Zapis i przechowywanie dodatkowych informacji o wersji zainstalowanego oprogramowania i zdalny odczyt tych informacji (wersja, zainstalowane uaktualnienia, sygnatury wirusów, itp.) z wbudowanej pamięci nieulotnej.-Technologia zarządzania i monitorowania komputerem na poziomie sprzętowym powinna być zgodna z otwartymi standardami DMTF WS-MAN (<http://www.dmtf.org/standards/wsman>) oraz DASH (<http://www.dmtf.org/standards/mgmt/dash/>). |
| Bezpieczeństwo | Płyta główna zawierająca układ sprzętowy służący do tworzenia i zarządzania wygenerowanymi przez komputer kluczami szyfrowania. Zabezpieczenie to musi posiadać możliwość szyfrowania poufnych dokumentów przechowywanych na dysku twardym przy użyciu klucza sprzętowegoZaimplementowany w BIOS system diagnostyczny z graficznym interfejsem użytkownika dostępny z poziomu BIOS lub szybkiego menu boot’owania, umożliwiający przetestowanie w celu wykrycia usterki zainstalowanych komponentów bez konieczności uruchamiania systemu operacyjnego. System musi posiadać wszystkie swoje funkcjonalności w przypadku: braku dysku, uszkodzenia dysku, sformatowania dysku, braku dostępu do sieci, internetu. Nie dopuszcza się stosowania wewnętrznych i zewnętrznych urządzeń w celu uzyskania funkcjonalności systemu diagnostycznego. Czujnik otwarcia obudowy, musi zbierać zdarzenia i zapisywać je w BIOS  |
| BIOS | BIOS zgodny ze specyfikacją UEFI, wyprodukowany przez producenta komputera, zawierający logo producenta komputera lub nazwę producenta komputera lub nazwę modelu oferowanego komputera. Pełna obsługa BIOS za pomocą klawiatury i myszy oraz samej myszy. BIOS wyposażony w automatyczną detekcję zmiany konfiguracji, automatycznie nanoszący zmiany w konfiguracji w szczególności: procesor, wielkość pamięci, pojemność dysku. Możliwość, bez uruchamiania systemu operacyjnego z dysku twardego komputera, bez dodatkowego oprogramowania (w tym również systemu diagnostycznego) i podłączonych do niego urządzeń zewnętrznych odczytania z BIOS informacji o: wersji BIOS, nr seryjnym komputera, ilości zainstalowanej pamięci RAM, prędkości zainstalowanych pamięci RAM, technologii wykonania pamięci, sposobie obsadzeniu slotów pamięci z rozbiciem na wielkości pamięci i banki, typie zainstalowanego procesora, ilości rdzeni zainstalowanego procesora, typowej prędkości zainstalowanego procesora, minimalnej i maksymalnej osiąganej prędkości zainstalowanego procesora, pojemności zainstalowanego lub zainstalowanych dysków twardych, wszystkich urządzeniach podpiętych do dostępnych na płycie głównej portów SATA, MAC adresie zintegrowanej karty sieciowej, zintegrowanym układzie graficznym, kontrolerze audio.Do odczytu wskazanych informacji nie mogą być stosowane rozwiązania oparte o pamięć masową (wewnętrzną lub zewnętrzną), zaimplementowane poza systemem BIOS narzędzia, np. system diagnostyczny, dodatkowe oprogramowanie.Funkcja blokowania/odblokowania BOOT-owania stacji roboczej z zewnętrznych urządzeń, możliwość ustawienia hasła systemowego/użytkownika umożliwiającego uruchomienie komputera (zabezpieczenie przed nieautoryzowanym uruchomieniem) przy jednoczesnym zdefiniowanym haśle administratora. Użytkownik po wpisaniu hasła systemowego/użytkownika w BIOS jest wstanie zidentyfikować ustawienia oraz dokonać zmiany hasła systemowego/użytkownika. Możliwość ustawienia haseł użytkownika i administratora składających się z cyfr, małych liter, dużych liter oraz znaków specjalnych. Możliwość ustawienia portów USB w trybie „no BOOT” (podczas startu komputer nie wykrywa urządzeń bootujących typu USB). Możliwość wyłączania portów USB pojedynczo. Dedykowane pole inwentarzowe umożliwiająca wpisanie oznaczenia sprzętu. Pole po nadaniu numeru nie może być edytowalne.Oferowany BIOS musi posiadać poza swoją wewnętrzną strukturą menu szybkiego boot’owania które umożliwia m.in.: uruchamianie systemu zainstalowanego na dysku twardym, uruchamianie systemu z urządzeń zewnętrznych, uruchamianie systemu z serwera za pośrednictwem zintegrowanej karty sieciowej, uruchomienie graficznego systemu diagnostycznego, wejście do BIOS, upgrade BIOS. |
| Certyfikaty i standardy | Certyfikat ISO9001 dla producenta sprzętu (załączyć do oferty)Certyfikat ISO 50001 dla producenta sprzętu (załączyć do oferty)Deklaracja zgodności CE (załączyć do oferty)Potwierdzenie spełnienia kryteriów środowiskowych, w tym zgodności z dyrektywą RoHS Unii Europejskiej o eliminacji substancji niebezpiecznych w postaci oświadczenia producenta jednostki (wg wytycznych Krajowej Agencji Poszanowania Energii S.A., zawartych w dokumencie „Opracowanie propozycji kryteriów środowiskowych dla produktów zużywających energię możliwych do wykorzystania przy formułowaniu specyfikacji na potrzeby zamówień publicznych”, pkt. 3.4.2.1; dokument z grudnia 2006), w szczególności zgodności z normą ISO 1043-4 dla płyty głównej oraz elementów wykonanych z tworzyw sztucznych o masie powyżej 25 gramCertyfikat TCO - do oferty załączyć certyfikat lub wydruk ze strony <http://tcocertified.com/product-finder/>  |
| Ergonomia | Głośność jednostki centralnej mierzona zgodnie z normą ISO 7779 oraz wykazana zgodnie z normą ISO 9296 w pozycji operatora w trybie pracy jałowej dysku twardego (IDLE) wynosząca maksymalnie 24 dB. |
| System operacyjny | System operacyjny klasy PC musi spełniać następujące wymagania poprzez wbudowane mechanizmy, bez użycia dodatkowych aplikacji:1. Dostępne dwa rodzaje graficznego interfejsu użytkownika:
2. klasyczny, umożliwiający obsługę przy pomocy klawiatury i myszy,
3. dotykowy umożliwiający sterowanie dotykiem na urządzeniach typu tablet lub monitorach dotykowych
4. Funkcje związane z obsługą komputerów typu tablet, z wbudowanym modułem „uczenia się” pisma użytkownika – obsługa języka polskiego
5. Interfejs użytkownika dostępny w wielu językach do wyboru – w tym polskim i angielskim
6. Możliwość tworzenia pulpitów wirtualnych, przenoszenia aplikacji pomiędzy pulpitami i przełączanie się pomiędzy pulpitami za pomocą skrótów klawiaturowych lub GUI.
7. Wbudowane w system operacyjny minimum dwie przeglądarki Internetowe
8. Zintegrowany z systemem moduł wyszukiwania informacji (plików różnego typu, tekstów, metadanych) dostępny z kilku poziomów: poziom menu, poziom otwartego okna systemu operacyjnego; system wyszukiwania oparty na konfigurowalnym przez użytkownika module indeksacji zasobów lokalnych,
9. Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, pomoc, komunikaty systemowe, menedżer plików.
10. Graficzne środowisko instalacji i konfiguracji dostępne w języku polskim
11. Wbudowany system pomocy w języku polskim.
12. Możliwość przystosowania stanowiska dla osób niepełnosprawnych (np. słabo widzących).
13. Możliwość dokonywania aktualizacji i poprawek systemu poprzez mechanizm zarządzany przez administratora systemu Zamawiającego.
14. Możliwość dostarczania poprawek do systemu operacyjnego w modelu peer-to-peer.
15. Możliwość sterowania czasem dostarczania nowych wersji systemu operacyjnego, możliwość centralnego opóźniania dostarczania nowej wersji o minimum 4 miesiące.
16. Zabezpieczony hasłem hierarchiczny dostęp do systemu, konta i profile użytkowników zarządzane zdalnie; praca systemu w trybie ochrony kont użytkowników.
17. Możliwość dołączenia systemu do usługi katalogowej on-premise lub w chmurze.
18. Umożliwienie zablokowania urządzenia w ramach danego konta tylko do uruchamiania wybranej aplikacji - tryb "kiosk".
19. Możliwość automatycznej synchronizacji plików i folderów roboczych znajdujących się na firmowym serwerze plików w centrum danych z prywatnym urządzeniem, bez konieczności łączenia się z siecią VPN z poziomu folderu użytkownika zlokalizowanego w centrum danych firmy.
20. Zdalna pomoc i współdzielenie aplikacji – możliwość zdalnego przejęcia sesji zalogowanego użytkownika celem rozwiązania problemu z komputerem.
21. Transakcyjny system plików pozwalający na stosowanie przydziałów (ang. quota) na dysku dla użytkowników oraz zapewniający większą niezawodność i pozwalający tworzyć kopie zapasowe.
22. Oprogramowanie dla tworzenia kopii zapasowych (Backup); automatyczne wykonywanie kopii plików z możliwością automatycznego przywrócenia wersji wcześniejszej.
23. Możliwość przywracania obrazu plików systemowych do uprzednio zapisanej postaci.
24. Możliwość przywracania systemu operacyjnego do stanu początkowego z pozostawieniem plików użytkownika.
25. Możliwość blokowania lub dopuszczania dowolnych urządzeń peryferyjnych za pomocą polityk grupowych (np. przy użyciu numerów identyfikacyjnych sprzętu)."
26. Wbudowany mechanizm wirtualizacji typu hypervisor."
27. Wbudowana możliwość zdalnego dostępu do systemu i pracy zdalnej z wykorzystaniem pełnego interfejsu graficznego.
28. Dostępność bezpłatnych biuletynów bezpieczeństwa związanych z działaniem systemu operacyjnego.
29. Wbudowana zapora internetowa (firewall) dla ochrony połączeń internetowych, zintegrowana z systemem konsola do zarządzania ustawieniami zapory i regułami IP v4 i v6.
30. Identyfikacja sieci komputerowych, do których jest podłączony system operacyjny, zapamiętywanie ustawień i przypisywanie do min. 3 kategorii bezpieczeństwa (z predefiniowanymi odpowiednio do kategorii ustawieniami zapory sieciowej, udostępniania plików itp.).
31. Możliwość zdefiniowania zarządzanych aplikacji w taki sposób aby automatycznie szyfrowały pliki na poziomie systemu plików. Blokowanie bezpośredniego kopiowania treści między aplikacjami zarządzanymi a niezarządzanymi.
32. Wbudowany system uwierzytelnienia dwuskładnikowego oparty o certyfikat lub klucz prywatny oraz PIN lub uwierzytelnienie biometryczne.
33. Wbudowane mechanizmy ochrony antywirusowej i przeciw złośliwemu oprogramowaniu z zapewnionymi bezpłatnymi aktualizacjami.
34. Wbudowany system szyfrowania dysku twardego ze wsparciem modułu TPM
35. Możliwość tworzenia i przechowywania kopii zapasowych kluczy odzyskiwania do szyfrowania dysku w usługach katalogowych.
36. Możliwość tworzenia wirtualnych kart inteligentnych.
37. Wsparcie dla firmware UEFI i funkcji bezpiecznego rozruchu (Secure Boot)
38. Wbudowany w system, wykorzystywany automatycznie przez wbudowane przeglądarki filtr reputacyjny URL.
39. Wsparcie dla IPSEC oparte na politykach – wdrażanie IPSEC oparte na zestawach reguł definiujących ustawienia zarządzanych w sposób centralny.
40. Mechanizmy logowania w oparciu o:
41. login i hasło,
42. karty inteligentne i certyfikaty (smartcard),
43. wirtualne karty inteligentne i certyfikaty (logowanie w oparciu o certyfikat chroniony poprzez moduł TPM),
44. certyfikat/Klucz i PIN
45. certyfikat/Klucz i uwierzytelnienie biometryczne
46. Wsparcie dla uwierzytelniania na bazie Kerberos v. 5
47. Wbudowany agent do zbierania danych na temat zagrożeń na stacji roboczej.
48. Wsparcie .NET Framework 2.x, 3.x i 4.x – możliwość uruchomienia aplikacji działających we wskazanych środowiskach
49. Wsparcie dla VBScript – możliwość uruchamiania interpretera poleceń
50. Wsparcie dla PowerShell 5.x – możliwość uruchamiania interpretera poleceń
 |
| Wymagania dodatkowe  | Wbudowane porty: 1x DP++ 1.4/HDCP 2.3 1x USB 3.2 Gen 2 Type-C port 3x USB 3.2 Gen 1 Type-A port 2x USB 2.0 Wymagane porty USB wbudowane, nie dopuszcza się stosowania rozgałęziaczy, hub’ów itp. Wszystkie porty dostępne dla użytkownika w najniższej możliwej regulacji wysokości 1x Universal audio jack 1x Line-out audio 1x RJ-45 port 10/100/1000 MbpsCzytnik kart SD 4.0 Karta WiFi ax+ bluetooth 5.1Płyta główna zaprojektowana i wyprodukowana na zlecenie producenta komputera, trwale oznaczona logo producenta oferowanej jednostki, dedykowana dla danego urządzenia; wyposażona w min. 2 złącza DIMM z obsługą do 64GB pamięci RAM, min. 1 złącza M.2 2280 dla dysku twardego oraz 1 złącze M.2 karty WiFi**Klawiatura bezprzewodowa USB w układzie polski programisty** **Mysz bezprzewodowa optyczna USB z dwoma przyciskami oraz rolką (scroll)** Nagrywarka DVD +/-RW wbudowana w obudowie lub w podstawie standu |
| Dodatkowe oprogramowanie | Oprogramowanie producenta komputera z nieograniczoną czasowo licencją na użytkowanie umożliwiające:* upgrade i instalacje wszystkich sterowników, aplikacji dostarczonych w obrazie systemu operacyjnego producenta, BIOS’u z certyfikatem zgodności producenta do najnowszej dostępnej wersji,
* sprawdzenie przed zainstalowaniem wszystkich sterowników, aplikacji oraz BIOS bezpośrednio na stronie producenta przy użyciu połączenia internetowego z automatycznym przekierowaniem w celu uzyskania informacji o: poprawkach i usprawnieniach dotyczących aktualizacji, dacie wydania ostatniej aktualizacji, priorytecie aktualizacji, zgodności z systemami operacyjnymi
* dostęp do wykazu najnowszych aktualizacji z podziałem na krytyczne (wymagające natychmiastowej instalacji), rekomendowane i opcjonalne
* włączenie/wyłączenie funkcji automatycznego restartu w przypadku, kiedy jest wymagany przy instalacji sterownika, aplikacji
* sprawdzenie historii aktualizacji z informacją, jakie sterowniki były instalowane z dokładną datą i wersją (rewizja wydania)
* dostęp do wykaz wymaganych sterowników, aplikacji, BIOS’u z informacją o zainstalowanej obecnie wersji dla oferowanego komputera z możliwością exportu do pliku o rozszerzeniu \*.xml
* dostęp do raportu uwzględniającego informacje o znalezionych, pobranych i zainstalowanych aktualizacjach z informacją, jakich komponentów dotyczyły, możliwość exportu takiego raportu do pliku \*.xml

Raport musi zawierać datę i godzinę podjętych i wykonanych akcji/zadań w przedziale czasowym min. 1 roku.**W ofercie należy podać nazwę oprogramowania.** |
| Wsparcie techniczne i gwarancja | Dedykowany portal techniczny producenta, umożliwiający Zamawiającemu zgłaszanie awarii oraz samodzielne zamawianie zamiennych komponentów. Możliwość sprawdzenia kompletnych danych o urządzeniu na jednej witrynie internetowej prowadzonej przez producenta (automatyczna identyfikacja komputera, konfiguracja fabryczna, konfiguracja bieżąca, Rodzaj gwarancji, data wygaśnięcia gwarancji, data produkcji komputera, aktualizacje, diagnostyka, dedykowane oprogramowanie, tworzenie dysku recovery systemu operacyjnego) 5-letnia gwarancja producenta świadczona na miejscu u klienta, Czas reakcji serwisu - do końca następnego dnia roboczego.W przypadku awarii dysków twardych dysk pozostaje u Zamawiającego. Firma serwisująca musi posiadać ISO 9001:2015 na świadczenie usług serwisowych oraz posiadać autoryzacje producenta komputera – dokumenty potwierdzające załączyć do oferty.Serwis urządzeń musi być realizowany przez Producenta lub Autoryzowanego Partnera Serwisowego Producenta. |

* 1. **Laptop – 1 szt.**

|  |  |
| --- | --- |
| **Parametr lub warunek**  | **Minimalne wymagania**  |
| Typ | Komputer przenośny typu laptop.**W ofercie wymagane jest podanie modelu producenta komputera.** |
| Zastosowanie | Komputer będzie wykorzystywany dla potrzeb aplikacji biurowych, aplikacji edukacyjnych, aplikacji obliczeniowych, dostępu do Internetu oraz poczty elektronicznej, jako lokalna baza danych, stacja programistyczna |
| Wydajność | Procesor wielordzeniowy zaprojektowany do pracy w komputerach przenośnych klasy x86.Procesor 64 bitowy o architekturze x86, o wydajności min. 13000 pkt w teście CPU Mark zgodnie z https://www.cpubenchmark.net/cpu\_list.php**Wykonawca w składanej ofercie winien podać dokładny model oferowanego podzespołu.** |
| Pamięć operacyjna | 8GB możliwość rozbudowy do min 32GB, 2 sloty na pamięci w tym min. jeden wolny |
| Pamięć masowa | 500GB NVMe SSD M.2 Fabrycznie dostosowane miejsce do instalacji drugiego dysku M.2  |
| Grafika | Grafika zintegrowana z procesorem powinna umożliwiać pracę min. dwumonitorową, współdzielona i dynamicznie przydzielana pamięć z RAM,  |
| Ekran | 15.6” FHD (1920 x 1080), powłoką przeciwodblaskową, jasność 250 nits, kontrast 700:1, NTSC 45%  |
| Multimedia | Karta dźwiękowa zintegrowana z płytą główną, wbudowane dwa głośniki stereo o mocy 2x 2W. Dwa kierunkowe, cyfrowe mikrofony z funkcją redukcji szumów i poprawy mowy wbudowane w obudowę matrycy.Kamera internetowa z diodą informującą o aktywności, 0.9 Mpix, trwale zainstalowana w obudowie matrycy wyposażona w mechaniczną przysłonę.czytnik kart micro SD, 1 port audio typu combo (słuchawki i mikrofon) |
| Obudowa | Szkielet obudowy i zawiasy notebooka wzmacniane, dookoła matrycy uszczelnienie chroniące klawiaturę notebooka, po zamknięciu przed kurzem i wilgocią. Kąt otwarcia notebooka min 180 stopni.Komputer spełniający normy MIL-STD-810H.Zasilacz o mocy min. 65W. |
| Zgodność z systemami operacyjnymi i standardami | Oferowane modele komputerów muszą poprawnie współpracować z zamawianymi systemami operacyjnymi (jako potwierdzenie poprawnej współpracy Wykonawca dołączy do oferty dokument w postaci wydruku potwierdzający certyfikację rodziny produktów bez względu na rodzaj obudowy, dodatkowo potwierdzony przez producenta oferowanego komputera). |
| Zarządzanie  | Wbudowana w płytę główną technologia zarządzania i monitorowania komputerem na poziomie sprzętowym działająca niezależnie od stanu czy obecności systemu operacyjnego oraz stanu włączenia komputera podczas pracy na zasilaczu sieciowym AC, obsługująca zdalną komunikację sieciową w oparciu o protokół IPv4 oraz IPv6, a także zapewniająca:monitorowanie konfiguracji komponentów komputera - CPU, Pamięć, HDD wersja BIOS płyty głównej; zdalną konfigurację ustawień BIOS,zdalne przejęcie konsoli tekstowej systemu, przekierowanie procesu ładowania systemu operacyjnego z wirtualnego CD ROM lub FDD z serwera zarządzającego;zdalne przejecie pełnej konsoli graficznej systemu tzw. KVM Redirection (Keyboard, Video, Mouse) bez udziału systemu operacyjnego ani dodatkowych programów, również w przypadku braku lub uszkodzenia systemu operacyjnego do rozdzielczości 1920x1080 włącznie;zapis i przechowywanie dodatkowych informacji o wersji zainstalowanego oprogramowania i zdalny odczyt tych informacji (wersja, zainstalowane uaktualnienia, sygnatury wirusów, itp.) z wbudowanej pamięci nieulotnej.technologia zarządzania i monitorowania komputerem na poziomie sprzętowym powinna być zgodna z otwartymi standardami DMTF WS-MAN (<http://www.dmtf.org/standards/wsman>) oraz DASH (<http://www.dmtf.org/standards/mgmt/dash/>)nawiązywanie przez sprzętowy mechanizm zarządzania, zdalnego szyfrowanego protokołem SSL/TLS połączenia z predefiniowanym serwerem zarządzającym, w definiowanych odstępach czasu, w przypadku wystąpienia predefiniowanego zdarzenia lub błędu systemowego (tzw. platform event) oraz na żądanie użytkownika z poziomu BIOS.wbudowany sprzętowo log operacji zdalnego zarządzania, możliwy do kasowania tylko przez upoważnionego użytkownika systemu sprzętowego zarządzania zdalnego sprzętowy firewall zarządzany i konfigurowany wyłącznie z serwera zarządzania oraz niedostępny dla lokalnego systemu OS i lokalnych aplikacjiw pełni aktywna konsola zarządzania wyświetlająca informacje i zachowująca pełną funkcjonalność nawet podczas restartów komputera zarządzanego.  |
| Bezpieczeństwo | Zintegrowany z płytą główną dedykowany układ sprzętowy służący do tworzenia i zarządzania wygenerowanymi przez komputer kluczami szyfrowania. Próba usunięcia układu powoduje uszkodzenie płyty głównej. Zabezpieczenie to musi posiadać możliwość szyfrowania poufnych dokumentów przechowywanych na dysku twardym przy użyciu klucza sprzętowego. Weryfikacja wygenerowanych przez komputer kluczy szyfrowania musi odbywać się w dedykowanym chipsecie na płycie głównej.Wbudowany czyjnik otwarcia obudowy (dolnej pokrywy)Czytnik linii papilarnych Czytnik SmartCard System diagnostyczny z graficznym interfejsem użytkownika zaszyty w tej samej pamięci flash co BIOS, dostępny z poziomu szybkiego menu boot lub BIOS, umożliwiający przetestowanie komputera a w szczególności jego składowych. Działający w pełni, bez okrojonych funkcjonalności nawet w przypadku uszkodzonego dysku, braku dysku lub sformatowanym dysku, dostępu do sieci i internetu oraz bez konieczności podłączenia urządzeń wewnętrznych i zewnętrznych. |
| BIOS | BIOS producenta oferowanego komputera zgodny ze specyfikacją UEFI, wymagana pełna obsługa za pomocą klawiatury i urządzenia wskazującego (wmontowanego na stałe) oraz samego urządzenia wskazującego. Możliwość, bez uruchamiania systemu operacyjnego z dysku twardego komputera lub innych, podłączonych do niego urządzeń zewnętrznych odczytania z BIOS informacji, oraz posiadać: datę produkcji komputera (data produkcji nieusuwalna), o kontrolerze audio, procesorze, a w szczególności min. i max. osiągana prędkość, pamięci RAM z informacją o taktowaniu i obsadzeniu w slotach. Niezmazywalne (nieedytowalne) pole asset tag z możliwością wpisywania min. znaków specjalnych. Funkcje logowania się do BIOS na podstawie hasła systemowego/użytkownika, administratora (hasła niezależne), Blokowanie hasłem systemowym/użytkownika dostępu do dysku twardego, funkcja umożliwiająca założenie hasła na dysk, informację o stanie naładowania baterii (stanu użycia), podpiętego zasilacza, zarządzanie trybem ładowania baterii (np. określenie docelowego poziomu naładowania). Możliwość nadania numeru inwentarzowego z poziomu BIOS bez wykorzystania dodatkowego oprogramowania, jak i konieczności aktualizacji BIOS.Możliwość włączenia/wyłączenia funkcji automatycznego tworzenia recovery BIOS na dysku twardym. |
| Certyfikaty i standardy | Certyfikat ISO9001 dla producenta sprzętu (należy załączyć do oferty)Certyfikat ISO 14001 dla producenta sprzętu (należy załączyć do oferty)Certyfikat ISO 50001 dla producenta sprzętu (należy załączyć do oferty)Deklaracja zgodności CE (załączyć do oferty)Potwierdzenie spełnienia kryteriów środowiskowych, w tym zgodności z dyrektywą RoHS Unii Europejskiej o eliminacji substancji niebezpiecznych w postaci oświadczenia producenta jednostkiPotwierdzenie kompatybilności komputera z oferowanym systemem operacyjnym (wydruk ze strony) |
| Ergonomia | Głośność jednostki centralnej mierzona zgodnie z normą ISO 7779 oraz wykazana zgodnie z normą ISO 9296 w pozycji obserwatora w trybie pracy dysku twardego (IDLE) wynosząca maksymalnie 19dB. |
| System operacyjny | System operacyjny klasy PC musi spełniać następujące wymagania poprzez wbudowane mechanizmy, bez użycia dodatkowych aplikacji:1. Dostępne dwa rodzaje graficznego interfejsu użytkownika:
2. klasyczny, umożliwiający obsługę przy pomocy klawiatury i myszy,
3. dotykowy umożliwiający sterowanie dotykiem na urządzeniach typu tablet lub monitorach dotykowych
4. Funkcje związane z obsługą komputerów typu tablet, z wbudowanym modułem „uczenia się” pisma użytkownika – obsługa języka polskiego
5. Interfejs użytkownika dostępny w wielu językach do wyboru – w tym polskim i angielskim
6. Możliwość tworzenia pulpitów wirtualnych, przenoszenia aplikacji pomiędzy pulpitami i przełączanie się pomiędzy pulpitami za pomocą skrótów klawiaturowych lub GUI.
7. Wbudowane w system operacyjny minimum dwie przeglądarki Internetowe
8. Zintegrowany z systemem moduł wyszukiwania informacji (plików różnego typu, tekstów, metadanych) dostępny z kilku poziomów: poziom menu, poziom otwartego okna systemu operacyjnego; system wyszukiwania oparty na konfigurowalnym przez użytkownika module indeksacji zasobów lokalnych,
9. Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, pomoc, komunikaty systemowe, menedżer plików.
10. Graficzne środowisko instalacji i konfiguracji dostępne w języku polskim
11. Wbudowany system pomocy w języku polskim.
12. Możliwość przystosowania stanowiska dla osób niepełnosprawnych (np. słabo widzących).
13. Możliwość dokonywania aktualizacji i poprawek systemu poprzez mechanizm zarządzany przez administratora systemu Zamawiającego.
14. Możliwość dostarczania poprawek do systemu operacyjnego w modelu peer-to-peer.
15. Możliwość sterowania czasem dostarczania nowych wersji systemu operacyjnego, możliwość centralnego opóźniania dostarczania nowej wersji o minimum 4 miesiące.
16. Zabezpieczony hasłem hierarchiczny dostęp do systemu, konta i profile użytkowników zarządzane zdalnie; praca systemu w trybie ochrony kont użytkowników.
17. Możliwość dołączenia systemu do usługi katalogowej on-premise lub w chmurze.
18. Umożliwienie zablokowania urządzenia w ramach danego konta tylko do uruchamiania wybranej aplikacji - tryb "kiosk".
19. Możliwość automatycznej synchronizacji plików i folderów roboczych znajdujących się na firmowym serwerze plików w centrum danych z prywatnym urządzeniem, bez konieczności łączenia się z siecią VPN z poziomu folderu użytkownika zlokalizowanego w centrum danych firmy.
20. Zdalna pomoc i współdzielenie aplikacji – możliwość zdalnego przejęcia sesji zalogowanego użytkownika celem rozwiązania problemu z komputerem.
21. Transakcyjny system plików pozwalający na stosowanie przydziałów (ang. quota) na dysku dla użytkowników oraz zapewniający większą niezawodność i pozwalający tworzyć kopie zapasowe.
22. Oprogramowanie dla tworzenia kopii zapasowych (Backup); automatyczne wykonywanie kopii plików z możliwością automatycznego przywrócenia wersji wcześniejszej.
23. Możliwość przywracania obrazu plików systemowych do uprzednio zapisanej postaci.
24. Możliwość przywracania systemu operacyjnego do stanu początkowego z pozostawieniem plików użytkownika.
25. Możliwość blokowania lub dopuszczania dowolnych urządzeń peryferyjnych za pomocą polityk grupowych (np. przy użyciu numerów identyfikacyjnych sprzętu)."
26. Wbudowany mechanizm wirtualizacji typu hypervisor."
27. Wbudowana możliwość zdalnego dostępu do systemu i pracy zdalnej z wykorzystaniem pełnego interfejsu graficznego.
28. Dostępność bezpłatnych biuletynów bezpieczeństwa związanych z działaniem systemu operacyjnego.
29. Wbudowana zapora internetowa (firewall) dla ochrony połączeń internetowych, zintegrowana z systemem konsola do zarządzania ustawieniami zapory i regułami IP v4 i v6.
30. Identyfikacja sieci komputerowych, do których jest podłączony system operacyjny, zapamiętywanie ustawień i przypisywanie do min. 3 kategorii bezpieczeństwa (z predefiniowanymi odpowiednio do kategorii ustawieniami zapory sieciowej, udostępniania plików itp.).
31. Możliwość zdefiniowania zarządzanych aplikacji w taki sposób aby automatycznie szyfrowały pliki na poziomie systemu plików. Blokowanie bezpośredniego kopiowania treści między aplikacjami zarządzanymi a niezarządzanymi.
32. Wbudowany system uwierzytelnienia dwuskładnikowego oparty o certyfikat lub klucz prywatny oraz PIN lub uwierzytelnienie biometryczne.
33. Wbudowane mechanizmy ochrony antywirusowej i przeciw złośliwemu oprogramowaniu z zapewnionymi bezpłatnymi aktualizacjami.
34. Wbudowany system szyfrowania dysku twardego ze wsparciem modułu TPM
35. Możliwość tworzenia i przechowywania kopii zapasowych kluczy odzyskiwania do szyfrowania dysku w usługach katalogowych.
36. Możliwość tworzenia wirtualnych kart inteligentnych.
37. Wsparcie dla firmware UEFI i funkcji bezpiecznego rozruchu (Secure Boot)
38. Wbudowany w system, wykorzystywany automatycznie przez wbudowane przeglądarki filtr reputacyjny URL.
39. Wsparcie dla IPSEC oparte na politykach – wdrażanie IPSEC oparte na zestawach reguł definiujących ustawienia zarządzanych w sposób centralny.
40. Mechanizmy logowania w oparciu o:
41. login i hasło,
42. karty inteligentne i certyfikaty (smartcard),
43. wirtualne karty inteligentne i certyfikaty (logowanie w oparciu o certyfikat chroniony poprzez moduł TPM),
44. certyfikat/Klucz i PIN
45. certyfikat/Klucz i uwierzytelnienie biometryczne
46. Wsparcie dla uwierzytelniania na bazie Kerberos v. 5
47. Wbudowany agent do zbierania danych na temat zagrożeń na stacji roboczej.
48. Wsparcie .NET Framework 2.x, 3.x i 4.x – możliwość uruchomienia aplikacji działających we wskazanych środowiskach
49. Wsparcie dla VBScript – możliwość uruchamiania interpretera poleceń
50. Wsparcie dla PowerShell 5.x – możliwość uruchamiania interpretera poleceń
 |
| Wymagania dodatkowe | Wbudowane porty i złącza: 1x HDMI 2.0, 1x RJ-45, 2x USB 3.2 w tym jeden port z zasilaniem, 2x Thunderbolt 4, złącze na linkę zabezpieczającą.Karta Wi-Fi 6 AC + Bluetooth 5.1 Modem LTE (opcjonalnie)Klawiatura z wydzieloną klawiaturą numeryczną i wbudowanym w klawiaturze podświetleniem, min 99 klawiszy. Wszystkie klawisze funkcyjne typu: mute, regulacja głośności, print screen dostępne w ciągu klawiszy F1-F12 |
| Oprogramowanie dodatkowe | Dołączone do oferowanego komputera oprogramowanie producenta z nieograniczoną licencją czasowo na użytkowanie umożliwiające:1. upgrade i instalacje wszystkich sterowników, aplikacji dostarczonych w obrazie systemu operacyjnego producenta, BIOS’u z certyfikatem zgodności producenta do najnowszej dostępnej wersji,
2. możliwość przed instalacją sprawdzenia każdego sterownika, każdej aplikacji, BIOS’u bezpośrednio na stronie producenta przy użyciu połączenia internetowego z automatycznym przekierowaniem a w szczególności informacji:
* poprawkach i usprawnieniach dotyczących aktualizacji
* dacie wydania ostatniej aktualizacji
* priorytecie aktualizacji
* zgodność z systemami operacyjnymi
* jakiego komponentu sprzętu dotyczy aktualizacja
* wszystkie poprzednie aktualizacje z informacjami jak powyżej.
1. wykaz najnowszych aktualizacji z podziałem na krytyczne (wymagające natychmiastowej instalacji), rekomendowane i opcjonalne
2. możliwość włączenia/wyłączenia funkcji automatycznego restartu w przypadku kiedy jest wymagany przy instalacji sterownika, aplikacji która tego wymaga.
3. rozpoznanie modelu oferowanego komputera, numer seryjny komputera, informację kiedy dokonany został ostatnio upgrade w szczególności z uwzględnieniem daty (dd-mm-rrrr)
4. sprawdzenia historii upgrade’u z informacją jakie sterowniki były instalowane z dokładną datą (dd-mm-rrrr ) i wersją (rewizja wydania)
5. dokładny wykaz wymaganych sterowników, aplikacji, BIOS’u z informacją o zainstalowanej obecnie wersji dla oferowanego komputera z możliwością exportu do pliku o rozszerzeniu \*.xml
6. raport uwzględniający informacje o: sprawdzaniu aktualizacji, znalezionych aktualizacjach, ściągniętych aktualizacjach, zainstalowanych aktualizacjach z dokładnym rozbiciem jakich komponentów to dotyczyło, błędach podczas sprawdzania, instalowania oraz możliwość exportu takiego raportu do pliku \*.xml od razu spakowany z rozszerzeniem \*.zip. Raport musi zawierać z dokładną datą (dd-mm-rrrr) i godziną z podjętych i wykonanych akcji/zadań w przedziale czasowym do min. 1 roku.
 |
| Wsparcie techniczne i gwarancja | Dedykowany portal techniczny producenta, umożliwiający Zamawiającemu zgłaszanie awarii oraz samodzielne zamawianie zamiennych komponentów. Możliwość sprawdzenia kompletnych danych o urządzeniu na jednej witrynie internetowej prowadzonej przez producenta (automatyczna identyfikacja komputera, konfiguracja fabryczna, konfiguracja bieżąca, Rodzaj gwarancji, data wygaśnięcia gwarancji, data produkcji komputera, aktualizacje, diagnostyka, dedykowane oprogramowanie, tworzenie dysku recovery systemu operacyjnego), 5-letnia gwarancja producenta świadczona na miejscu u klienta, Czas reakcji serwisu - do końca następnego dnia roboczego.W przypadku awarii dysków twardych dysk pozostaje u Zamawiającego.Firma serwisująca musi posiadać ISO 9001:2015 na świadczenie usług serwisowych oraz posiadać autoryzacje producenta komputera – dokumenty potwierdzające załączyć do oferty.Serwis urządzeń musi być realizowany przez Producenta lub Autoryzowanego Partnera Serwisowego Producenta. |

* 1. **Urządzenie wielofunkcyjne A3 kolor – 1 szt.**

|  |  |
| --- | --- |
| **Parametr lub****warunek** | **Minimalne wymagania** |
| **Typ urządzenia** | Urządzenie wielofunkcyjne: drukarka kolorowa, kopiarka kolorowa, skaner kolorowy **W ofercie wymagane jest podanie modelu producenta urządzenia.** |
| **Prędkość druku** | mono i kolor min.  23 stron A4 na minutę simplex / duplex                         min. 10 stron A3 na minutę  |
| **Technologia druku** | laserowa kolorowa C,M,Y,K  |
| **Maksymalny format papieru** | nie mniejszy niż A3  |
| **Czas nagrzewania** | nie więcej niż 18 sekund  |
| **Czas wykonania pierwszej kopii** | nie więcej niż 6,2 sekund mono, nie więcej niż 8,2 sekundy kolor  |
| **Wejściowa obsługa papieru** | co najmniej 2 kasety uniwersalne o pojemności nie mniejszej niż 500 arkuszy każda, taca ręczna o pojemności nie mniejszej niż 100 arkuszy  |
| **Obsługiwana gramatura papieru** | co najmniej w zakresie od 60 do 256 g/m2  |
| **Automatyczny podajnik dokumentów** | wymagany, z funkcją odwracania, o pojemności nie mniejszej niż 100 arkuszy, obsługujący formaty A6-A3; w gramaturze 35-163 g/m²  |
| **Funkcja zoom** | co najmniej w zakresie od 25-400% w odstępach 0.1%; automatyczne powiększenie  |
| **Kopiowanie wielokrotne** | co najmniej w zakresie 1 - 9,999  |
| **Zainstalowana pamięć** | min. 3,0 GB RAM oraz twardy dysk SSD o pojemności min. 240 GB  |
| **Język drukarki** | PCL6 (wer.3.0), PostScript3 (3016), XPS wer.1.0, wymagany oryginalny sterownik producenta urządzenia, interfejs sterownika druku z możliwością edytowania zakładki z ulubionymi opcjami, interfejs sterownika druku w języku polskim.  |
| **Zawansowane funkcje drukowania** | Aplikacja, która umożliwia drukowanie z pozycji komputera bez instalacji sterownika za pomocą „przeciąg i puść”.  Umożliwiająca: 1) Tworzenie Hot folderów do bezpośredniego druku 2) Skojarzenie specyficznych ustawień z hot folderami  3)Automatyczne zapisywanie plików w folderach „druku” 4) Obsługuje PDF, TIFF, PCL i PS  |
| **Protokoły sieciowe** | TCP/IP, IPX/SPX,   |
| **Rozdzielczość kopiowania i skanowania** | nie mniejsza niż 600 x 600 dpi   |
| **Rozdzielczość drukowania** | Nie mniejsza niż 1,800 x 600   |
| **Interfejsy** | USB 2.0, 10/100/1000BaseTX  |
| **Funkcje drukarki** | bezpośredni druk PDF, bezpośredni druk z pamięci USB  |
| **Tryby skanera** | Scan-to-USB, Scan-to-Me, Skan-to-SMB, Scan-to-Home, Scan-to-FTP, Scan-to-Box, Scan-to-USB, Scan-to-WebDAV, Scan-to-DPWS, Network TWAIN scan. Adnotacje (tekst/godzina/data) w plikach PDF; Pomijanie pustych stron. Podgląd i edycja zeskanowanych obrazów przed wysłaniem/zapisaniem.  |
| **Wyjściowe formaty plików skanera** | JPEG; TIFF; PDF; PDF/A; kompaktowy PDF; szyfrowany PDF; XPS; kompaktowy XPS; PPTX;  |
| **Szafka pod urządzenie** | Wymagana, metalowa na kółkach. Zamawiający wymaga szafki w kolorach odpowiadającym kolorom urządzenia  |
| **Funkcje monitorująco raportujące** | Aplikacja umożliwiająca poprzez przeglądarkę internetową, dodawanie użytkowników (do 1000 kont użytkowników; obsługa również Active Directory (login + hasło + e-mail + katalog SMB)) z możliwością definiowania uprawnień do danych funkcji urządzenia np.  Wydruku: mono / kolor, Kopia Mono / Kolor Skanowanie. Rozwiązanie winno umożliwiać również możliwość raportowania ilości wykonanych wydruków / kopii / skanów, poszczególnych użytkowników wpisanych do systemu. System musi posiadać autoryzacje użytkowania na maszynie za pomocą: Login i hasła domenowego za pomocą którego można zwalniać wydruki z serwera urządzenia. |
| **Wymagane funkcje bezpieczeństwa** | ISO 15408 EAL3; zgodność z IEEE 2600.1; filtrowanie IP i blokowanie portów; komunikacja sieciowa SSL2; SSL3 i TSL1.0; obsługa IPsec; obsługa IEEE 802.1x; uwierzytelnianie użytkowników; dziennik uwierzytelniania; bezpieczne drukowanie; nadpisywanie dysku twardego (8 metod); szyfrowanie danych na dysku twardym (AES 128); automatyczne usuwanie danych z pamięci; szyfrowanie danych druku użytkownika;  |
| **Materiały eksploatacyjne** | Toner czarny dostarczony z urządzeniem pozwalający na wydrukowanie minimum 23.000 stron A4 przy zadruku 5% oraz tonery cyan, magenta, yellow dostarczone z urządzeniem pozwalające na wydrukowanie minimum 23.000 stron A4 przy zadruku 5%,   |
| **Instalacja** | Zamawiający wymaga w cenie uruchomienia wyżej opisanego urządzenia oraz wdrożenia systemów zawansowanych funkcji drukowania oraz skanowania w skazanym miejscu przez Zamawiającego.  |
| **Wymagane certyfikaty** | **Certyfikat ISO 27001** - System Zarządzania Bezpieczeństwem Informacji w Organizacji - Sprzedaż urządzeń wielofunkcyjnych i biurowych, projektowanie, sprzedaż i wdrażanie rozwiązań informatycznych do zarządzania procesem druku, obiegiem dokumentacji. Dostarczanie usług serwisowych do urządzeń wielofunkcyjnych, biurowych, drukarek, urządzeń poligraficznych oraz rozwiązań informatycznych.  Certyfikat wydany przez Jednostkę zrzeszoną w IAF - International Accreditation Forum. **Certyfikat ISO 20000** – System Zarządzania Usługami IT w Organizacji - Sprzedaż urządzeń wielofunkcyjnych i biurowych, projektowanie, sprzedaż i wdrażanie rozwiązań informatycznych do zarządzania procesem druku, obiegiem dokumentacji. Dostarczanie usług serwisowych do urządzeń wielofunkcyjnych, biurowych, drukarek, urządzeń poligraficznych oraz rozwiązań informatycznych. Certyfikat wydany przez Jednostkę zrzeszoną w IAF - International Accreditation Forum.  |
| **Wymagania gwarancji.** | Urządzenie winno mieć wykupiony min 24 miesięcznym pakiet gwarancji producenta sprzętu. Zamawiający nie dopuszcza gwarancji wystawionej przez subdystrybutora, dealera czy też brokera.   |
| **Wymagane dokumenty** | Urządzenie musi być fabrycznie nowe. Przed dostawą sprzęt musi być zarejestrowany przez producenta, bezpośrednio na Zamawiającego, jako jedynego użytkownika po opuszczeniu fabryki. Jeśli producent nie prowadzi rejestracji sprzętu, to wymaga się deklaracji producenta, iż sprzęt jest fabrycznie nowy. Sprzęt musi pochodzić z autoryzowanego przez jej producenta kanału dystrybucji w UE i nie może być obciążony uprzednio nabytymi prawami podmiotów trzecich    |

1. **Oprogramowanie biurowe i antywirusowe.**

**2.1. Oprogramowanie biurowe dla stacji roboczych – 19 lic.**

1) Zamawiający wymaga dostarczenia licencji wieczystej oprogramowania w najnowszej na dzień składania ofert wersji, wyposażonego w następujące wbudowane funkcjonalności, bez użycia dodatkowych aplikacji:

1. dostępność pakietu w wersjach 32-bit oraz 64-bit, stały dostęp do najnowszych aktualizacji zakupionej wersji oprogramowania,
2. możliwość dostosowania dokumentów i szablonów do potrzeb użytkownika, oraz narzędzia umożliwiające dystrybucję odpowiednich szablonów do właściwych odbiorców
3. możliwość zintegrowania uwierzytelniania użytkowników z usługą katalogową (Active Directory lub funkcjonalnie równoważną) - użytkownik raz zalogowany z poziomu systemu operacyjnego stacji roboczej ma być automatycznie rozpoznawany we wszystkich modułach oferowanego rozwiązania bez potrzeby oddzielnego monitowania go o ponowne uwierzytelnienie się.

 2) Wymagania odnośnie interfejsu użytkownika:

* 1. Pełna polska wersja językowa interfejsu użytkownika.
	2. Prostota i intuicyjność obsługi, pozwalająca na pracę osobom nieposiadającym umiejętności technicznych.

3) Oprogramowanie musi umożliwiać tworzenie i edycję dokumentów elektronicznych w ustalonym standardzie, który spełnia następujące warunki:

* 1. posiada kompletny i publicznie dostępny opis formatu,
	2. ma zdefiniowany układ informacji w postaci XML zgodnie z Załącznikiem 2 Rozporządzenia Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (Dz.U. 2012, poz. 526 ze zm.),
	3. umożliwia kreowanie plików w formacie XML,
	4. wspiera w swojej specyfikacji podpis elektroniczny w formacie XAdES,

4) W skład oprogramowania muszą wchodzić narzędzia programistyczne umożliwiające automatyzację pracy i wymianę danych pomiędzy dokumentami i aplikacjami (język makropoleceń, język skryptowy).

5) Do aplikacji musi być dostępna pełna dokumentacja w języku polskim.

6) Pakiet zintegrowanych aplikacji biurowych musi zawierać nieograniczone czasowo ani funkcjonalnie następujące składowe:

* 1. Edytor tekstów,
	2. Arkusz kalkulacyjny,
	3. Narzędzie do przygotowywania i prowadzenia prezentacji,
	4. Narzędzie do zarządzania informacją prywatną,

Zabezpieczenie dokumentów hasłem przed odczytem oraz przed wprowadzaniem modyfikacji.

7) Arkusz kalkulacyjny musi umożliwiać:

* 1. Tworzenie raportów tabelarycznych
	2. Tworzenie wykresów liniowych (wraz linią trendu), słupkowych, kołowych
	3. Tworzenie arkuszy kalkulacyjnych zawierających teksty, dane liczbowe oraz formuły przeprowadzające operacje matematyczne, logiczne, tekstowe, statystyczne oraz operacje na danych finansowych i na miarach czasu.
	4. Tworzenie raportów z zewnętrznych źródeł danych (inne arkusze kalkulacyjne, bazy danych zgodne z ODBC, pliki tekstowe, pliki XML, webservice)
	5. Obsługę kostek OLAP oraz tworzenie i edycję kwerend bazodanowych i webowych. Narzędzia wspomagające analizę statystyczną i finansową, analizę wariantową i rozwiązywanie problemów optymalizacyjnych
	6. Tworzenie raportów tabeli przestawnych umożliwiających dynamiczną zmianę wymiarów oraz wykresów bazujących na danych z tabeli przestawnych
	7. Wyszukiwanie i zamianę danych
	8. Wykonywanie analiz danych przy użyciu formatowania warunkowego
	9. Tworzenie wykresów prognoz i trendów na podstawie danych historycznych z użyciem algorytmu ETS
	10. Nazywanie komórek arkusza i odwoływanie się w formułach po takiej nazwie
	11. Nagrywanie, tworzenie i edycję makr automatyzujących wykonywanie czynności
	12. Formatowanie czasu, daty i wartości finansowych z polskim formatem
	13. Zapis wielu arkuszy kalkulacyjnych w jednym pliku.
	14. Inteligentne uzupełnianie komórek w kolumnie według rozpoznanych wzorców, wraz z ich możliwością poprawiania poprzez modyfikację proponowanych formuł.
	15. Możliwość przedstawienia różnych wykresów przed ich finalnym wyborem (tylko po najechaniu znacznikiem myszy na dany rodzaj wykresu).

Zachowanie pełnej zgodności z formatami plików utworzonych za pomocą oprogramowania Microsoft Excel 2010, 2013, 2016, 2019, 365 z uwzględnieniem poprawnej realizacji użytych w nich funkcji specjalnych i makropoleceń.

1. Zabezpieczenie dokumentów hasłem przed odczytem oraz przed wprowadzaniem modyfikacji

8) Narzędzie do przygotowywania i prowadzenia prezentacji musi umożliwiać:

a. Przygotowywanie prezentacji multimedialnych, które będą:

- Prezentowanie przy użyciu projektora multimedialnego

- Drukowanie w formacie umożliwiającym robienie notatek

b. Zapisanie, jako prezentacja tylko do odczytu.

c. Nagrywanie narracji i dołączanie jej do prezentacji

d. Opatrywanie slajdów notatkami dla prezentera

e. Umieszczanie i formatowanie tekstów, obiektów graficznych, tabel, nagrań dźwiękowych i wideo

f. Umieszczanie tabel i wykresów pochodzących z arkusza kalkulacyjnego

g. Odświeżenie wykresu znajdującego się w prezentacji po zmianie danych w źródłowym arkuszu kalkulacyjnym

h. Możliwość tworzenia animacji obiektów i całych slajdów

i. Prowadzenie prezentacji w trybie prezentera, gdzie slajdy są widoczne na jednym monitorze lub projektorze, a na drugim widoczne są slajdy i notatki prezentera, z możliwością podglądu następnego slajdu.

j. Pełna zgodność z formatami plików utworzonych za pomocą oprogramowania MS PowerPoint 2010, 2013, 2016, 2019 i 365.

9) Narzędzie do zarządzania informacją prywatną (pocztą elektroniczną, kalendarzem, kontaktami i zadaniami) musi umożliwiać:

a. Pobieranie i wysyłanie poczty elektronicznej z serwera pocztowego,

b. Przechowywanie wiadomości na serwerze lub w lokalnym pliku tworzonym z

zastosowaniem efektywnej kompresji danych,

c. Filtrowanie niechcianej poczty elektronicznej (SPAM) oraz określanie listy zablokowanych i bezpiecznych nadawców,

d. Tworzenie katalogów, pozwalających katalogować pocztę elektroniczną,

e. Automatyczne grupowanie poczty o tym samym tytule,

f. Tworzenie reguł przenoszących automatycznie nową pocztę elektroniczną do określonych katalogów bazując na słowach zawartych w tytule, adresie nadawcy i odbiorcy,

g. Oflagowanie poczty elektronicznej z określeniem terminu przypomnienia, oddzielnie dla nadawcy i adresatów,

h. Mechanizm ustalania liczby wiadomości, które mają być synchronizowane lokalnie,

i. Zarządzanie kalendarzem,

j. Udostępnianie kalendarza innym użytkownikom z możliwością określania uprawnień użytkowników,

k. Przeglądanie kalendarza innych użytkowników,

l. Zapraszanie uczestników na spotkanie, co po ich akceptacji powoduje automatyczne wprowadzenie spotkania w ich kalendarzach,

m. Zarządzanie listą zadań,

n. Zlecanie zadań innym użytkownikom,

o. Zarządzanie listą kontaktów,

p. Udostępnianie listy kontaktów innym użytkownikom,

q. Przeglądanie listy kontaktów innych użytkowników,

r. Możliwość przesyłania kontaktów innym użytkowników,

s. Możliwość wykorzystania do komunikacji z serwerem pocztowym mechanizmu MAPI poprzez http.

**2.2. Oprogramowanie antywirusowe dla stacji roboczych – 19 lic.**

W ramach licencji wieczystej z min. 2-letnim dostępem w szczególności do najnowszych wersji oprogramowania, baz sygnatur i wsparcia technicznego oprogramowanie musi spełniać następujące wymagania poprzez wbudowane mechanizmy, bez użycia dodatkowych aplikacji:

* musi wspierać systemy operacyjne Windows 10/Windows 11.
* musi wspierać architekturę 32 i 64-bitową systemu Windows.
* musi wspierać architekturę ARM64.
* musi być dostępne co najmniej w języku polskim oraz angielskim.
* Instalator rozwiązania musi umożliwiać wybór wersji językowej programu, przed rozpoczęciem procesu instalacji.
* Pomoc w rozwiązaniu (help) i dokumentacja rozwiązania dostępna co najmniej w języku polskim oraz angielskim.
* Skuteczność rozwiązania potwierdzona nagrodami VB100 i AV-comparatives.
* Rozwiązanie musi zapewniać pełną ochronę przed wirusami, trojanami, robakami i innymi zagrożeniami.
* Rozwiązanie musi zapewniać wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor.
* Rozwiązanie musi posiadać wbudowaną technologię do ochrony przed rootkitami.
* Rozwiązanie musi wykrywać potencjalnie niepożądane, niebezpieczne oraz podejrzane aplikacje.
* Rozwiązanie musi posiadać możliwość skanowanie w czasie rzeczywistym otwieranych, tworzonych i wykonywanych plików.
* Rozwiązanie musi posiadać możliwość skanowania całego dysku, wybranych katalogów, pojedynczych plików „na żądanie” lub według harmonogramu.
* Rozwiązanie musi posiadać możliwość definiowania zadań w harmonogramie, w taki sposób, aby zadanie przed wykonaniem sprawdzało czy komputer pracuje na zasilaniu bateryjnym, jeśli tak – nie wykonywało danego zadania.
* Rozwiązanie musi posiadać możliwość utworzenia wielu różnych zadań skanowania według harmonogramu (w tym: co godzinę, po zalogowaniu i po uruchomieniu komputera). Każde zadanie ma mieć możliwość uruchomienia z innymi ustawieniami (czyli metody skanowania, obiekty skanowania, czynności, rozszerzenia przeznaczone do skanowania, priorytet skanowania).
* Rozwiązanie musi posiadać opcję skanowania „na żądanie” pojedynczych plików lub katalogów przy pomocy skrótu w menu kontekstowym.
* Rozwiązanie musi posiadać możliwość określania priorytetu wykorzystania procesora (CPU) podczas skanowania „na żądanie” i według harmonogramu.
* Rozwiązanie musi posiadać możliwość skanowania dysków sieciowych i dysków przenośnych.Rozwiązanie musi posiadać możliwość skanowania plików spakowanych I skompresowanych.
* Rozwiązanie musi posiadać możliwość umieszczenia na liście wykluczeń ze skanowania wybranych plików, katalogów lub plików o określonych rozszerzeniach.
* Administrator musi mieć możliwość dodania wykluczenia dla zagrożenia po nazwie,
* sumie kontrolnej (SHA1) oraz lokalizacji pliku.
* Rozwiązanie musi posiadać możliwość automatycznego wyłączenia komputera po zakończonym skanowaniu.
* Rozwiązanie nie może wymagać ponownego uruchomienia (restartu) komputera po instalacji.
* Użytkownik musi posiadać możliwość tymczasowego wyłączenia ochrony na czas co najmniej 10 minut lub do ponownego uruchomienia komputera.
* W momencie tymczasowego wyłączenia ochrony antywirusowej użytkownik musi być poinformowany o takim fakcie odpowiednim powiadomieniem i informacją w interfejsie aplikacji.
* Ponowne włączenie ochrony antywirusowej nie może wymagać od użytkownika ponownego uruchomienia komputera.
* Rozwiązanie musi posiadać możliwość przeniesienia zainfekowanych plików i załączników poczty w bezpieczny obszar dysku (do katalogu kwarantanny) w celu dalszej kontroli. Pliki muszą być przechowywane w katalogu kwarantanny w postaci zaszyfrowanej.
* Rozwiązanie musi posiadać wbudowany konektor dla programów MS Outlook, Outlook Express, Windows Mail i Windows Live Mail.
* Rozwiązanie musi umożliwiać skanowanie i oczyszczanie w czasie rzeczywistym poczty przychodzącej i wychodzącej obsługiwanej przy pomocy programu MS Outlook, Outlook Express, Windows Mail i Windows Live Mail.
* Rozwiązanie musi umożliwiać 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).
* Rozwiązanie musi automatycznie integrować skaner POP3 i IMAP z dowolnym klientem pocztowym bez konieczności zmian w konfiguracji.
* Rozwiązanie musi posiadać możliwość opcjonalnego dołączenia informacji o przeskanowaniu do każdej odbieranej wiadomości e-mail lub tylko do zainfekowanych wiadomości e-mail.
* Rozwiązanie musi umożliwiać skanowanie ruchu HTTP na poziomie stacji roboczych. Zainfekowany ruch jest automatycznie blokowany, a użytkownikowi wyświetlane jest stosowne powiadomienie.
* Rozwiązanie musi posiadać możliwość blokowania możliwości przeglądania wybranych stron internetowych. Rozwiązanie musi umożliwić blokowanie danej strony internetowej po podaniu przynajmniej całego adresu URL strony lub części adresu URL.
* Rozwiązanie musi posiadać możliwość zdefiniowania blokady wszystkich stron internetowych z wyjątkiem listy stron, ustalonej przez administratora.
* Rozwiązanie musi automatycznie integrować się z dowolną przeglądarką internetową bez konieczności zmian w konfiguracji.
* Rozwiązanie musi umożliwiać skanowanie ruchu sieciowego wewnątrz szyfrowanych protokołów HTTPS, POP3S, IMAPS.
* Rozwiązanie musi zapewniać skanowanie ruchu szyfrowanego transparentnie bez potrzeby konfiguracji zewnętrznych aplikacji, takich jak: przeglądarki internetowe oraz programy pocztowe.
* Rozwiązanie musi posiadać możliwość zgłoszenia witryny z podejrzeniem phishingu z poziomu graficznego interfejsu użytkownika, w celu analizy przez laboratorium producenta.
* Administrator ma mieć możliwość zdefiniowania portów TCP, na których rozwiązanie będzie realizowało proces skanowania ruchu szyfrowanego.
* Rozwiązanie musi posiadać funkcjonalność, która na bieżąco będzie odpytywać serwery producenta o znane i bezpieczne procesy uruchomione na komputerze użytkownika.
* Procesy zweryfikowane jako bezpieczne mają być pomijane podczas procesu skanowania oraz przez moduły ochrony w czasie rzeczywistym.
* Użytkownik musi posiadać możliwość przesłania pliku celem zweryfikowania jego reputacji bezpośrednio z poziomu menu kontekstowego.
* W przypadku, gdy stacja robocza nie będzie posiadała dostępu do sieci Internet, ma odbywać się skanowanie wszystkich procesów, również tych, które wcześniej zostały uznane za bezpieczne.
* Rozwiązanie musi posiadać dwa wbudowane niezależne moduły heurystyczne – jeden wykorzystujący pasywne metody heurystyczne i drugi wykorzystujący aktywne metody heurystyczne oraz elementy sztucznej inteligencji. Musi istnieć możliwość wyboru z jaką heurystyką ma odbywać się skanowanie – z użyciem jednej lub obu metod jednocześnie.
* Rozwiązanie musi posiadać możliwość automatycznego wysyłania nowych zagrożeń do laboratoriów producenta bezpośrednio z programu (nie wymaga ingerencji użytkownika). Użytkownik musi mieć możliwość określenia rozszerzeń dla plików, które nie będą wysyłane automatycznie.
* Do wysłania próbki zagrożenia do laboratorium producenta, rozwiązanie nie może wykorzystywać klienta pocztowego zainstalowanego na komputerze użytkownika.
* Dane statystyczne zbierane przez producenta na podstawie otrzymanych próbek nowych zagrożeń mają być w pełni anonimowe.
* Rozwiązanie musi posiadać możliwość ręcznego wysłania próbki nowego zagrożenia z katalogu kwarantanny do laboratorium producenta.
* Rozwiązanie musi posiadać możliwość zabezpieczenia konfiguracji hasłem, aby każdy użytkownik przy próbie dostępu do konfiguracji, był proszony o jego podanie.
* Rozwiązanie musi posiadać możliwość zabezpieczenia przed deinstalacją przez niepowołaną osobę, nawet, gdy posiada ona prawa lokalnego lub domenowego administratora. Przy próbie deinstalacji rozwiązanie musi pytać o hasło.
* Hasło do zabezpieczenia konfiguracji rozwiązania oraz deinstalacji musi być takie samo.
* Rozwiązanie musi mieć możliwość kontroli zainstalowanych aktualizacji systemu operacyjnego i w przypadku braku aktualizacji – poinformować o tym użytkownika i wyświetlenia listy niezainstalowanych aktualizacji.
* Rozwiązanie musi mieć możliwość definiowania typu aktualizacji systemowych o braku, których będzie informował użytkownika w tym przynajmniej: aktualizacje krytyczne, aktualizacje ważne, aktualizacje zalecane oraz aktualizacje o niskim priorytecie. Ma być możliwość dezaktywacji tego mechanizmu.
* Po instalacji rozwiązania, użytkownik ma mieć możliwość przygotowania płyty CD, DVD lub pamięci USB, z której będzie w stanie uruchomić komputer w przypadku infekcji i przeskanować dysk w poszukiwaniu zagrożeń.
* System antywirusowy, uruchomiony z płyty bootowalnej lub pamięci USB, ma umożliwiać pełną aktualizację silnika detekcji z Internetu lub z bazy zapisanej na dysku.
* System antywirusowy, uruchomiony z płyty bootowalnej lub pamięci USB, ma pracować w trybie graficznym.
* Rozwiązanie musi posiadać umożliwiać 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.
* Funkcja blokowania nośników wymiennych, bądź grup urządzeń, ma umożliwiać użytkownikowi tworzenie reguł dla podłączanych urządzeń, minimum w oparciu o typ, numer seryjny, dostawcę oraz model urządzenia.
* Rozwiązanie musi mieć możliwość utworzenia reguły na podstawie podłączonego urządzenia. Dana funkcjonalność musi pozwalać na automatyczne wypełnienie typu, numeru seryjnego, dostawcy oraz modelu urządzenia.
* Rozwiązanie musi umożliwiać użytkownikowi nadanie uprawnień dla podłączanych urządzeń, w tym co najmniej: dostęp w trybie do odczytu, pełen dostęp, ostrzeżenie, brak dostępu do podłączanego urządzenia.
* Rozwiązanie musi posiadać funkcjonalność, umożliwiającą zastosowanie reguł dla podłączanych urządzeń w zależności od zalogowanego użytkownika.
* W momencie podłączenia zewnętrznego nośnika, rozwiązanie musi wyświetlić użytkownikowi odpowiedni komunikat i umożliwić natychmiastowe przeskanowanie całej zawartości podłączanego nośnika.
* Administrator ma posiadać możliwość takiej konfiguracji rozwiązania, aby skanowanie całego nośnika odbywało się automatycznie lub za potwierdzeniem przez użytkownika.
* Rozwiązanie musi być wyposażone w system zapobiegania włamaniom działający na hoście (HIPS).
* Moduł HIPS musi posiadać możliwość pracy w jednym z pięciu trybów:
* tryb automatyczny z regułami, gdzie program automatycznie tworzy i wykorzystuje reguły wraz z możliwością wykorzystania reguł utworzonych przez użytkownika,
* tryb interaktywny, w którym to rozwiązanie pyta użytkownika o akcję w przypadku wykrycia aktywności w systemie,
* tryb oparty na regułach, gdzie zastosowanie mają jedynie reguły utworzone przez użytkownika,
* 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,
* tryb inteligentny, w którym rozwiązanie będzie powiadamiało wyłącznie o szczególnie podejrzanych zdarzeniach.
* Tworzenie reguł dla modułu HIPS musi odbywać się co najmniej w oparciu o: aplikacje źródłowe, pliki docelowe, aplikacje docelowe, elementy docelowe rejestru systemowego.
* Użytkownik na etapie tworzenia reguł dla modułu HIPS musi posiadać możliwość wybrania jednej z trzech akcji: pytaj, blokuj, zezwól.
* Rozwiązanie musi posiadać zaawansowany skaner pamięci.
* Rozwiązanie musi być wyposażone w mechanizm ochrony przed exploitami w popularnych aplikacjach, przynajmniej czytnikach PDF, aplikacjach JAVA, przeglądarkach internetowych.
* 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.
* 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.
* Rozwiązanie musi posiadać posiadać funkcję, która aktywnie monitoruje wszystkie pliki programu, jego procesy, usługi i wpisy w rejestrze i skutecznie blokuje ich modyfikacje przez aplikacje trzecie.
* Rozwiązanie musi posiadać automatyczną, inkrementacyjną aktualizację silnika detekcji.
* Rozwiązanie musi posiadać możliwość utworzenia kilku zadań aktualizacji. Każde zadanie musi być uruchamiane przynajmniej z jedną z opcji: co godzinę, po zalogowaniu, po uruchomieniu komputera.
* Rozwiązanie musi posiadać możliwość określenia maksymalnego wieku dla silnika detekcji, po upływie którego rozwiązanie zgłosi posiadanie nieaktualnego silnika detekcji.
* Rozwiązanie musi posiadać funkcjonalność tworzenia lokalnego repozytorium aktualizacji modułów.
* Rozwiązanie musi posiadać funkcjonalność udostępniania tworzonego repozytorium aktualizacji modułów za pomocą wbudowanego w program serwera HTTP.
* Rozwiązanie musi być wyposażone w funkcjonalność, umożliwiającą tworzenie kopii wcześniejszych aktualizacji modułów w celu ich późniejszego przywrócenia (rollback).
* Rozwiązanie musi być wyposażone tylko w jeden proces uruchamiany w pamięci, z którego korzystają wszystkie funkcje systemu (antywirus, antyspyware, metody heurystyczne).
* Rozwiązanie musi posiadać funkcjonalność, która automatycznie wykrywa aplikacje pracujące w trybie pełnoekranowym.
* W momencie wykrycia trybu pełnoekranowego, rozwiązanie ma wstrzymać wyświetlanie wszystkich powiadomień związanych ze swoją pracą oraz wstrzymać zadania znajdujące się w harmonogramie zadań rozwiązania.
* Użytkownik ma mieć możliwość skonfigurowania po jakim czasie włączone mają zostać powiadomienia oraz zadania, pomimo pracy w trybie pełnoekranowym.
* Rozwiązanie musi być wyposażone w dziennik zdarzeń, rejestrujący informacje na temat znalezionych zagrożeń, kontroli dostępu do urządzeń, skanowania oraz zdarzeń.
* Rozwiązanie musi posiadać możliwość utworzenia dziennika diagnostycznego z poziomu interfejsu aplikacji.
* Rozwiązanie musi posiadać możliwość aktywacji przy użyciu co najmniej jednej z trzech metod: poprzez podanie poświadczeń administratora licencji, klucza licencyjnego lub aktywacji programu w trybie offline.
* Rozwiązanie musi mieć możliwość podejrzenia informacji o licencji, która znajduje się w programie.
* W trakcie instalacji rozwiązanie ma umożliwiać wybór komponentów, które mają być instalowane. Instalator ma zezwalać na wybór co najmniej następujących modułów do instalacji: kontrola dostępu do urządzeń, zapora osobista, ochrona poczty, ochrona protokołów, kontrola dostępu do stron internetowych, RMM.
* W rozwiązaniu musi istnieć możliwość tymczasowego wstrzymania działania polityk, wysłanych z poziomu serwera zdalnej administracji.
* Wstrzymanie polityk ma umożliwić lokalną zmianę ustawień rozwiązania na stacji końcowej.
* Funkcja wstrzymania polityki musi być realizowana tylko przez określony czas, po którym automatycznie zostaną przywrócone dotychczasowe ustawienia.
* Administrator ma możliwość wstrzymania polityk na 10 minut, 30 minut, 1 godzinę lub 4 godziny.
* Aktywacja funkcji wstrzymania polityki musi obsługiwać uwierzytelnienie za pomocą hasła lub konta użytkownika.
* Rozwiązanie musi posiadać opcję automatycznego skanowania komputera po wyłączeniu wstrzymania polityki.
* Rozwiązanie musi posiadać możliwość zmiany konfiguracji programu z poziomu dedykowanego modułu wiersza poleceń. Zmiana konfiguracji jest w takim przypadku autoryzowana bez hasła lub za pomocą hasła do ustawień zaawansowanych.
* Rozwiązanie musi posiadać możliwość definiowana stanów rozwiązania, jakie będą wyświetlane użytkownikowi, co najmniej: ostrzeżeń o wyłączonych mechanizmach ochrony czy stanie licencji.
* Administrator musi mieć możliwość dodania własnego komunikatu do stopki powiadomień, jakie będą wyświetlane użytkownikowi na pulpicie.
* Rozwiązanie musi posiadać funkcjonalność skanera UEFI, który chroni użytkownika poprzez wykrywanie i blokowanie zagrożeń, atakujących jeszcze przed uruchomieniem systemu operacyjnego.
* Wbudowany skaner UEFI nie może posiadać dodatkowego interfejsu graficznego i musi być transparentny dla użytkownika, aż do momentu wykrycia zagrożenia.
* Rozwiązanie musi posiadać dedykowany moduł, zapewniający ochronę przed oprogramowaniem wymuszającym okup.
* Administrator ma możliwość dodania wykluczenia dla procesu, wskazując plik wykonywalny.
* Rozwiązanie musi posiadać możliwość przeskanowania pojedynczego pliku, poprzez opcję „przeciągnij i upuść”.
* Administrator musi posiadać możliwość określenia typu podejrzanych plików, jakie będą przesyłane do producenta, w tym co najmniej pliki wykonywalne, archiwa, skrypty, dokumenty.
* Administrator musi posiadać możliwość wyłączenia z przesyłania do analizy producenta określonych plików i folderów.
* Rozwiązanie musi posiadać funkcjonalność umożliwiającą zastosowanie reguł dla podłączanych urządzeń w zależności od zdefiniowanego przedziału czasowego.
* Rozwiązanie musi posiadać wbudowany system IDS z detekcją prób ataków, anomalii w pracy sieci oraz wykrywaniem aktywności wirusów sieciowych.
* Rozwiązanie musi posiadać ochronę przed dołączeniem komputera do sieci botnet.
* Rozwiązanie musi posiadać ochronę przed atakami Brute-Force, która zablokuje próbę siłowego dostania się do stacji roboczej za pomocą protokołu RDP i SMB. 109.Rozwiązanie musi posiadać pełne wsparcie zarówno dla protokołu IPv4 jak i dla standardu IPv6.
* Wsparcie techniczne do programu świadczone w języku polskim przez polskiego dystrybutora, autoryzowanego przez producenta programu.
* Rozwiązanie musi posiadać ochronę antyspamową dla programów pocztowych MS Outlook, Outlook Express, Windows Mail oraz Windows Live Mail.
* Rozwiązanie musi umożliwiać wyłączenie skanowania baz programu pocztowego po zmianie zawartości skrzynki odbiorczej.
* Rozwiązanie musi umożliwiać automatyczne wpisanie do białej listy wszystkich kontaktów z książki adresowej programu pocztowego.
* Rozwiązanie musi posiadać możliwość ręcznej zmiany klasyfikacji wiadomości spamu na pożądaną lub niepożądaną bezpośrednio z klienta pocztowego.
* Rozwiązanie musi posiadać możliwość ręcznego dodania nadawcy wiadomości do białej lub czarnej listy bezpośrednio z klienta pocztowego.
* Rozwiązanie musi posiadać możliwość definiowania folderu, gdzie program pocztowy będzie umieszczać spam.
* Rozwiązanie musi możliwość zdefiniowania dowolnego tekstu, dodawanego do tematu wiadomości zakwalifikowanej jako spam.
* Rozwiązanie musi domyślnie współpracować z folderem „Wiadomości-śmieci”, dostępnym w programie Microsoft Outlook.
* Rozwiązanie ma umożliwiać funkcjonalność, która po zmianie klasyfikacji wiadomości typu spam na pożądaną, oznaczy ją jako „nieprzeczytana”
* Rozwiązanie ma umożliwiać funkcjonalność, która po zmianie klasyfikacji wiadomości pożądanej na spam oznaczy ją jako „przeczytana”.
* Rozwiązanie musi posiadać funkcjonalność wyłączenia modułu antyspamowego na określony czas lub do czasu ponownego uruchomienia komputera.
* Zapora osobista rozwiązania musi pracować w jednym z czterech trybów:
	+ tryb automatyczny – rozwiązanie blokuje cały ruch przychodzący i zezwala tylko na połączenia wychodzące,
	+ tryb interaktywny – rozwiązanie pyta się o każde nowo nawiązywane połączenie,
	+ tryb oparty na regułach – rozwiązanie blokuje cały ruch przychodzący i wychodzący, zezwalając tylko na połączenia skonfigurowane przez administratora,
	+ tryb uczenia się – rozwiązanie automatycznie tworzy nowe reguły zezwalające na połączenia przychodzące i wychodzące. Administrator musi posiadać możliwość konfigurowania czasu działania trybu.
* Rozwiązanie musi oceniać reguły zapory systemu Windows.
* Rozwiązanie musi posiadać możliwość tworzenia list sieci zaufanych.
* Rozwiązanie musi posiadać możliwość dezaktywacji funkcji zapory sieciowej poprzez trwałe wyłączenie.
* Rozwiązanie musi posiadać możliwość określenia w regułach zapory osobistej kierunku ruchu, portu lub zakresu portów, protokołu, aplikacji, usługi i adresu lub zakresu adresów komputera lokalnego lub/i zdalnego.
* Rozwiązanie musi posiadać możliwość wyboru jednej z trzech akcji w trakcie tworzenia reguł w trybie interaktywnym: zezwól, zablokuj i pytaj.
* Rozwiązanie musi posiadać możliwość powiadomienia użytkownika o nawiązaniu określonych połączeń oraz odnotowanie faktu nawiązania danego połączenia w dzienniku zdarzeń aplikacji.
* Rozwiązanie musi posiadać możliwość zdefiniowania wielu niezależnych zestawów reguł dla każdej sieci, w której pracuje komputer, w tym minimum dla strefy zaufanej i sieci Internet.
* Rozwiązanie musi wykrywać modyfikację w aplikacjach, korzystających z sieci I powiadamianie o tym zdarzeniu.
* Rozwiązanie musi posiadać możliwość tworzenia profili pracy zapory osobistej w zależności od wykrytej sieci.
* Administrator ma możliwość sprecyzowania, który profil zapory ma zostać zaaplikowany po wykryciu danej sieci.
* Profile mają możliwość automatycznego przełączania, bez ingerencji użytkownika lub administratora.
* Autoryzacja stref ma się odbywać min. w oparciu o: zaaplikowany profil połączenia, adres serwera DNS, sufiks domeny, adres domyślnej bramy, adres serwera WINS, adres serwera DHCP, lokalny adres IP, identyfikator SSID, szyfrowania sieci bezprzewodowej lub jego brak, konkretny interfejs sieciowy w systemie.
* Podczas konfiguracji autoryzacji sieci, administrator ma mieć możliwość definiowania adresów IP dla lokalnego połączenia, adresu IP serwera DHCP, adresu serwera DNS oraz adresu IP serwera WINS, zarówno z wykorzystaniem adresów IPv4 jak i IPv6.
* Opcje związane z autoryzacją stref mają posiadać możliwość łączenia (np. lokalnego adresu IP z adresem serwera DNS) w dowolnej kombinacji, celem zwiększenia dokładności identyfikacji danej sieci.
* Rozwiązanie musi posiadać kreator, który umożliwia rozwiązywanie problemów z połączeniem. Musi pozwalać na rozwiązanie problemów:
	+ z aplikacją lokalną, którą administrator wskazuje z listy,
	+ z połączeniem z urządzeniem zdalnym, na podstawie jego adresu IP.
* Rozwiązanie musi być wyposażone w zintegrowany moduł kontroli dostępu do stron internetowych.
* Moduł kontroli dostępu do stron internetowych musi posiadać możliwość utworzenia reguł w oparciu o użytkownika lub grupę użytkowników systemu Windows lub Active Directory.
* Rozwiązanie musi posiadać możliwość filtrowania adresów URL w oparciu o co najmniej 140 kategorii i podkategorii.
* Podstawowe kategorie, w jakie rozwiązanie musi być wyposażone to: materiały dla dorosłych, usługi biznesowe, komunikacja i sieci społecznościowe, działalność przestępcza, oświata, rozrywka, gry, zdrowie, informatyka, styl życia, aktualności, polityka, religia i prawo, wyszukiwarki, bezpieczeństwo i szkodliwe oprogramowanie, zakupy, hazard, udostępnianie plików, zainteresowania dzieci, serwery proxy, alkohol i tytoń, szukanie pracy, nieruchomości, finanse i pieniądze, niebezpieczne sporty, nierozpoznane kategorie oraz elementy niezaliczone do żadnej kategorii.
* Moduł musi posiadać możliwość grupowania kategorii oraz adresów stron internetowych.
* Lista adresów URL znajdujących się w poszczególnych kategoriach, musi być automatycznie aktualizowana przez producenta.
* Administrator musi posiadać możliwość wyłączenia integracji modułu kontroli dostępu do stron internetowych.
* Rozwiązanie musi posiadać możliwość określenia przynajmniej jednej z akcji dla reguły kontroli dostępu do stron internetowych: zezwól, ostrzeż, blokuj.
* Rozwiązanie musi posiadać także możliwość dodania komunikatu i grafiki w przypadku zablokowania, określonej w regułach, strony internetowej.
* Rozwiązanie musi być wyposażona w moduł bezpiecznej przeglądarki.
* Przeglądarka musi automatycznie szyfrować wszelkie dane wprowadzane przez Użytkownika. Użytkownik w momencie wejścia na stronę, która znajduje się na liści chronionych witryn, musi automatycznie zostać przekierowany do okna bezpiecznej przeglądarki.
* Administrator musi mieć możliwość konfiguracji listy chronionych witryn, przez bezpieczną przeglądarkę.
* Administrator musi mieć możliwość konfiguracji, aby użytkownik przy próbie dostępu do strony bankowości elektronicznej, automatycznie został przekierowany do okna bezpiecznej przeglądarki.
* Praca w bezpiecznej przeglądarce musi być wyróżniona poprzez odpowiedni kolor ramki przeglądarki oraz informację na ramce przeglądarki.
* Serwer administracyjny musi posiadać możliwość instalacji na systemach Windows Server
* 2012, 2016, 2019 oraz systemach Linux.
* Serwer zarządzający musi być dostępny w postaci gotowej maszyny wirtualnej w formacie OVA (Open Virtual Appliance) oraz dysku wirtualnego w formacie VHD.
* Serwer administracyjny musi wspierać instalację z użyciem nowego lub istniejącego serwera bazy danych MS SQL i MySQL.
* Konsola administracyjna musi umożliwiać podgląd szczegółów, dotyczących bazy danych takich jak: serwer, nazwa, aktualny rozmiar, nazwa hosta, użytkownik.
* Serwer administracyjny musi posiadać możliwość konfiguracji zadania cyklicznego czyszczenia bazy danych.
* Administrator musi posiadać możliwość pobrania wszystkich wymaganych elementów serwera centralnej administracji w postaci jednego pakietu instalacyjnego i każdego z modułów oddzielnie bezpośrednio ze strony producenta.
* Dostęp do konsoli centralnego zarządzania musi odbywać się z poziomu interfejsu WWW.
* Narzędzie administracyjne musi wspierać połączenia poprzez serwer proxy.
* Narzędzie administracyjne musi być kompatybilne z protokołami IPv4 oraz IPv6.
* Podczas logowania do konsoli, administrator musi mieć możliwość wyboru języka, w jakim zostanie wyświetlony interfejs.
* Zmiana języka interfejsu konsoli nie może wymagać jej zatrzymania, ani reinstalacji.
* Interfejs musi być zabezpieczony za pośrednictwem protokołu SSL.
* Konsola administracyjna musi ostrzegać administratora, kiedy używa niewspieranej przeglądarki, do administracji rozwiązaniem antywirusowym.
* Narzędzie do administracji zdalnej musi posiadać moduł, pozwalający na wykrycie niezarządzanych stacji roboczych w sieci.
* Serwer administracyjny musi posiadać mechanizm instalacji zdalnej agenta na stacjach roboczych.
* Serwer administracyjny musi posiadać mechanizm wykrywający sklonowane maszyny na podstawie unikatowego identyfikatora sprzętowego stacji.
* Serwer administracyjny musi posiadać wsparcie dla „VDI” oraz „Golden Master Image”.
* Serwer administracyjny musi posiadać możliwość podłączenia 250 000 hostów.
* Instalacja serwera administracyjnego powinna posiadać możliwość pracy w sieci rozproszonej, nie wymagając dodatkowego serwera proxy.
* Rozwiązanie ma posiadać możliwość komunikacji agenta przy wykorzystaniu HTTP Proxy.
* Administrator musi posiadać możliwość instalacji modułu do zarządzania urządzeniami mobilnymi – MDM.
* Serwer administracyjny musi posiadać możliwość sprawdzenia lokalizacji dla urządzeń z systemami iOS.
* Serwer administracyjny musi posiadać możliwość wdrożenia urządzenia z iOS z wykorzystaniem programu DEP.
* Serwer administracyjny musi posiadać możliwość konfiguracji polityk zabezpieczeń takich jak: ograniczenia funkcji urządzenia, blokadę usuwania aplikacji, konfigurację usługi Airprint, konfigurację ustawień Bluetooth, Wi-Fi, VPN dla urządzeń z systemem iOS 10 oraz 11.
* Serwer administracyjny musi posiadać możliwość lokalizacji urządzeń mobilnych przy wykorzystaniu Google maps, Bing maps, OpenStreetMap.
* Administrator musi posiadać możliwość instalacji serwera HTTP Proxy, pozwalającego na pobieranie aktualizacji silnika detekcji oraz pakietów instalacyjnych na stacjach roboczych.
* Serwer HTTP Proxy musi posiadać mechanizm zapisywania w pamięci podręcznej (cache) pobieranych elementów.
* Komunikacja pomiędzy poszczególnymi modułami serwera musi być zabezpieczona za pomocą certyfikatów.
* Serwer administracyjny musi posiadać możliwość utworzenia własnego CA (Certification Authority) oraz dowolnej liczby certyfikatów z podziałem na typ elementu: agent, serwer zarządzający, serwer proxy, moduł zarządzania urządzeniami mobilnymi.
* Serwer administracyjny musi pozwalać na zarządzanie programami zabezpieczającymi na maszynach z systemami Windows, MacOS, Linux, Android.
* Serwer administracyjny musi pozwalać na zarządzanie urządzeniami z systemem iOS.
* Serwer administracyjny musi pozwalać na centralną konfigurację i zarządzanie przynajmniej takimi modułami jak: ochrona antywirusowa, zapora osobista, kontrola dostępu do stron internetowych, które działają na stacjach roboczych w sieci.
* Zarządzanie oprogramowaniem zabezpieczającym na stacjach roboczych musi odbywać się za pośrednictwem dedykowanego agenta.
* Administrator musi posiadać możliwość zarządzania stacjami roboczymi za pomocą dedykowanego agenta, na których nie jest zainstalowane oprogramowanie zabezpieczające.
* Z poziomu konsoli zarządzania administrator ma mieć możliwość weryfikacji podzespołów zarządzanego komputera (w tym przynajmniej: producent, model, numer seryjny, typ i wersja oprogramowania układowego, informacje o systemie, procesor, pamięć RAM, wykorzystanie dysku twardego, informacje o wyświetlaczu, urządzenia peryferyjne, urządzenia audio, drukarki, karty sieciowe, urządzenia masowe) oraz wylistowanie zainstalowanego oprogramowania firm trzecich dla systemów Windows oraz MacOS z możliwością jego odinstalowania.
* Serwer administracyjny musi posiadać możliwość wymuszenia połączenia agenta do serwera administracyjnego z pominięciem domyślnego czasu oczekiwania na połączenie.
* Instalacja zdalna agenta z poziomu serwera administracyjnego nie może wymagać określenia architektury systemu (32 lub 64 bitowy) oraz jego rodzaju (Windows, MacOS, Linux), a wybór odpowiedniego pakietu musi być w pełni automatyczny.
* W przypadku braku zainstalowanego produktu zabezpieczającego na urządzeniu mobilnym z systemem Android, musi istnieć możliwość jego pobrania ze sklepu Google Play.
* Administrator musi posiadać możliwość utworzenia listy autoryzowanych urządzeń mobilnych, które mogą zostać podłączone do serwera centralnej administracji.
* Serwer administracyjny musi posiadać możliwość zablokowania, odblokowania, wyczyszczenia zawartości, zlokalizowania oraz uruchomienia syreny na zarządzanym urządzaniu mobilnym. Funkcjonalność musi wykorzystywać połączenie internetowe, a nie komunikację za pośrednictwem wiadomości SMS.
* Administrator musi posiadać możliwość utworzenia użytkownika serwera administracyjnego.
* Administrator musi posiadać możliwość dodania grupy użytkowników z Active Directory do serwera administracyjnego. Użytkownik grupy usługi katalogowej Active Directory musi mieć możliwość logowania się do konsoli administracyjnej swoimi poświadczeniami domenowymi.
* Administrator musi posiadać możliwość wymuszenia dwufazowej autoryzacji podczas logowania do konsoli administracyjnej.
* Serwer administracyjny musi posiadać możliwość dodania zestawu uprawnień dla użytkowników w oparciu co najmniej o funkcje zarządzania: politykami, instalacją agentów, raportowaniem, zarządzaniem licencjami, zadaniami administracyjnymi. Każda z funkcji musi posiadać możliwość wyboru uprawnienia: odczyt, użyj, zapisz oraz brak.
* Administrator musi posiadać możliwość przypisania kilku zestawów uprawnień do jednego użytkownika.
* Użytkownik musi posiadać możliwość zmiany hasła dla swojego konta, bez konieczności logowania się do konsoli administracyjnej.
* Serwer administracyjny musi posiadać możliwość konfiguracji czasu bezczynności, po którym użytkownik zostanie automatycznie wylogowany.
* Serwer administracyjny musi posiadać zadania klienta oraz zadania serwera. Zadania serwera muszą zawierać przynajmniej zadanie instalacji agenta, generowania raportów oraz synchronizacji elementów z Active Directory. Zadania klienta muszą być wykonywane za pośrednictwem agenta na stacji roboczej.
* Agent musi posiadać mechanizm pozwalający na zapis zadania w swojej pamięci wewnętrznej w celu ich późniejszego wykonania bez względu na stan połączenia z serwerem centralnej administracji.
* Serwer administracyjny musi posiadać możliwość instalacji oprogramowania z użyciem parametrów instalacyjnych.
* Serwer administracyjny musi posiadać możliwość deinstalacji programu zabezpieczającego firm trzecich, zgodnych z technologią OPSWAT.
* Serwer administracyjny musi posiadać możliwość wysłania polecenia: wyświetlenia komunikatu, aktualizacji systemu operacyjnego, zamknięcia komputera, uruchomienia ponownego komputera oraz uruchomienia komendy na stacji klienckiej.
* Serwer administracyjny musi posiadać możliwość uruchomienia zadania automatycznie, przynajmniej z wyzwalaczem: wyrażenie CRON, codziennie, cotygodniowo, comiesięcznie, corocznie, po wystąpieniu nowego zdarzenia oraz umieszczeniu agenta w grupie dynamicznej.
* Serwer administracyjny musi posiadać możliwość tworzenia grup statycznych i dynamicznych komputerów.
* 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.
* Serwer administracyjny musi posiadać możliwość utworzenia polityk dla programów zabezpieczających i komponentów środowiska serwera centralnego zarządzania.
* Serwer administracyjny musi posiadać możliwość przypisania polityki dla pojedynczego klienta lub dla grupy komputerów.
* Serwer administracyjny musi posiadać możliwość przypisania kilku polityk z innymi priorytetami dla pojedynczego klienta.
* Edytor konfiguracji polityki musi być identyczny jak edytor konfiguracji ustawień w programie zabezpieczającym na stacji roboczej.
* Serwer administracyjny musi umożliwiać wyświetlenie polityk, które są przypisane do stacji.
* Z poziomu konsoli musi istnieć możliwość scalania reguł zapory osobistej, harmonogramu, modułu HIPS z już istniejącymi regułami na stacji roboczej lub innej polityce.
* Serwer administracyjny musi posiadać minimum 120 szablonów raportów, przygotowanych przez producenta.
* Serwer administracyjny musi posiadać możliwość utworzenia własnych raportów.
* Serwer administracyjny musi posiadać możliwość wyboru formy przedstawienia danych w raporcie w tym przynajmniej: w postaci tabeli, wykresu lub obu elementów jednocześnie.
* Serwer administracyjny musi posiadać możliwość wyboru jednego z kilku typów wykresów: kołowy, pierścieniowy, liniowy, słupkowy, punktowy.
* Serwer administracyjny musi posiadać możliwość określenia danych, jakie powinny znajdować się w poszczególnych kolumnach tabeli lub na osiach wykresu oraz ich odfiltrowania i posortowania.
* Serwer administracyjny musi być wyposażony w mechanizm importu oraz eksportu szablonów raportów.
* Serwer administracyjny powinien posiadać panel kontrolny z raportami, pozwalający na szybki dostępu do najbardziej interesujących danych. Panel ten musi być edytowalny.
* Serwer administracyjny musi posiadać możliwość wygenerowania raportu na żądanie, zgodnie z harmonogramem lub umieszczenia raportu na panelu kontrolnym. Raport może zostać wysłany za pośrednictwem wiadomości email, zapisany do pliku w formacie PDF lub CSV.
* Raport na panelu kontrolnym musi być w pełni interaktywny, pozwalając przejść do zarządzania stacją/stacjami, której raport dotyczy.
* Serwer administracyjny musi posiadać możliwość utworzenia własnych powiadomień lub skorzystania z predefiniowanych wzorów.
* Powiadomienia mailowe mają być wysyłane w formacie HTML.
* Powiadomienia muszą być wywoływane po zmianie ilości członków danej grupy dynamicznej, wzroście liczby klientów grupy w stosunku do innej grupy, pojawienia się dziennika zagrożeń.
* Administrator musi posiadać możliwość wysłania powiadomienia przynajmniej za pośrednictwem wiadomości email, komunikatu SNMP oraz do dziennika syslog.
* Serwer administracyjny musi posiadać możliwość agregacji identycznych powiadomień występujących w zadanym przez administratora okresie czasu.
* Serwer administracyjny musi posiadać możliwość synchronizacji danych dotyczących licencji.
* Serwer administracyjny musi posiadać możliwość dodania licencji przynajmniej przy użyciu
* klucza licencyjnego, pliku offline licencji oraz konta systemu zarządzania licencjami.
* Serwer administracyjny musi posiadać możliwość dodania dowolnej ilości licencji produktów zarządzanych.
* W przypadku posiadania tylko jednej dodanej licencji w konsoli zarządzania ma być ona wybierana automatycznie podczas konfiguracji zadania aktywacji lub instalacji produktu.
* Serwer administracyjny musi posiadać możliwość weryfikacji identyfikatora publicznego licencji, ilości wykorzystanych stanowisk, czasu wygaśnięcia, wersji produktu, na który jest licencja oraz jej właściciela.
* Serwer administracyjny musi posiadać możliwość wybudzania stacji roboczych przy użyciu Wake on Lan.
* Serwer musi umożliwić podział uprawnień administratorów w taki sposób, aby każdy z nich miał możliwość zarządzania konkretnymi grupami komputerów, politykami oraz zadaniami.
* Serwer ma posiadać możliwość wygenerowania dziennika diagnostycznego na stacji roboczej, który może zostać pobrany bezpośrednio z konsoli.
* W szczegółach stacji roboczej, z poziomu konsoli, muszą być dostępne zaawansowane logi diagnostyczne, przynajmniej z modułów produktu zabezpieczającego, takich jak: antyspam, firewall, HIPS, kontrola dostępu do urządzeń, kontrola dostępu do stron internetowych.
* Konsola webowa musi zawierać informacje, dotyczące wysłanych plików do analizy producenta.
* Administrator musi mieć możliwość pobrania pliku z parametrami połączenia RDP do stacji roboczej bezpośrednio z poziomu konsoli.
* Na panelu kontrolnym musi być dostępny dziennik zmian, dotyczący produktów zabezpieczających i komponentów środowiska centralnego zarządzania.
* Serwer musi wspierać wysyłanie logów do systemu SIEM IBM qRadar w jego natywnym formacie.
* Konsola administracyjna musi umożliwiać personalizację interfejsu webowego.
* Konsola administracyjna musi mieć możliwość tagowania obiektów, w tym przynajmniej: polityki, zadania, komputery oraz szablony grupy dynamicznych.
* Konsola administracyjna musi mieć możliwość zarządzania rozwiązaniem do szyfrowania całej powierzchni dysku, które pochodzi od tego samego producenta oraz posiadać możliwość zarządzania natywnym szyfrowaniem dla systemów macOS (FileVault).
* Konsola administracyjna musi pozwalać na utworzenie wykluczeń globalnych, bez konieczności przypisywania ich do konkretnych polityk.
* Serwer administracyjny musi oferować możliwość bezpośredniego sprawdzenia SHA-1 pliku, wykrytego przez produkt antywirusowy, na portalach służących do weryfikacji bezpieczeństwa (co najmniej VirusTotal).
* Konsola administracyjna musi posiadać możliwość wyświetlania dziennika audytu czynności wykonanych przez administratorów serwera. Dziennik musi pozwalać na wyświetlanie informacji co najmniej ze zmian dotyczących: certyfikatów, zadań, wyzwalaczy, konfiguracji, grup, uprawnień administratorów, wykluczeń, powiadomień, raportów.
1. **Dostawa i instalacja oraz konfiguracja systemu składowania i archiwizacji danych oraz wykonywania kopii zapasowych**
	1. **Koncepcja wdrożenia**

Macierz dyskowa stanowi jeden z ważniejszych elementów infrastruktury IT ponieważ odpowiada za bezpieczeństwo przechowywania, przetwarzania oraz transmisji danych, w związku z tym rozwiązanie powinno spełniać wymagania określone w rozdziale IV rozporządzenia Rady Ministrów w sprawie Krajowych Ram Interoperacyjności, obowiązujących norm oraz standardów rynkowych.

Użytkowa przestrzeń dyskowa macierzy będzie wykorzystana na potrzeby:

1. Zapisu danych z systemów dziedzinowych i ich archiwizacja,
2. Przechowywania plików dziennika systemowego,
3. Udostępnienia przestrzeni na udziały współdzielone,

Należy dostarczyć serwer pamięci masowej (NAS) wraz z dyskami dużej pojemności oraz wysokiej dostępności, wyposażonego w dyski klasy Enterprise.

Macierz dyskowa powinna zapewnić bezpieczeństwo danych poprzez zastosowanie redundantnych komponentów takich jak dyski i zasilacze (typu hot plug). Przestrzeń dyskowa zostanie skonfigurowana w macierz RAID 1.

* 1. **Serwer NAS Tower – 1 szt.**

|  |  |
| --- | --- |
| **Parametr lub warunek** | **Minimalne wymagania techniczne i funkcjonalne dla macierzy dyskowej**  |
| **Obudowa**  | 1) Obudowa typu Tower.2) Obudowa powinna posiadać widoczne elementy sygnalizacyjne do informowania o stanie poprawnej pracy lub awarii/macierzy. 3) Macierz powinna dysponować przynajmniej jednym czterordzeniowym procesorem o nominalnej prędkości przynajmniej 2 GHz. |
| **Interfejsy**  | 1) Oferowana macierz musi mieć minimum 2 porty RJ-45 1GbE LAN 2) Macierz musi mieć możliwość rozbudowy o dodatkowe porty za pomocą karty rozszerzeń PCI-E |
| **Poziomy RAID**  | Macierz musi zapewniać poziom zabezpieczenia danych na dyskach definiowany poziomami RAID: 0, 1 , 5, 6, 1+0 |
| **Wspierane dyski**  | Oferowana macierz musi wspierać dyski:1) dyski technologii minimum SATA (3Gb/s), ~~wspierające operacje hot-plug prędkości obrotowej minimum 5400 obrotów na minutę,~~2) dyski elektroniczne SolidStateDrive wykonane w technologii hot-plug, 3) dyski elektroniczne w formacie 3,5” oraz 2,5”.4) przynajmniej 4 dyski  |
| **Zainstalowane dyski** | W macierzy musi być zainstalowanych 2 dyski o parametrach nie gorszych niż:1) Pojemność pojedynczego dysku minimum 10TB w formacie 3,5”.~~2) Prędkość obrotowa minimum 7200 rpm.~~  |
| **Opcje software’owe**  | 1) Oferowana macierz musi być wyposażona w system kopii migawkowych (snapshot) z licencją na minimum 2048 kopii migawkowych. 2) Macierz musi umożliwiać dokonywanie migracji danych ze zmianą poziomu RAID.3) Macierz musi posiadać wsparcie dla systemów operacyjnych: MS Windows Server 2008/2012, SuSE Linux, RedHat Linux, SUN Solaris, VMWare 5.x, Citrix XEN Server.4) Macierz musi obsługiwać mechanizmy Thin Provisioning, czyli przydziału dla obsługiwanych środowisk woluminów logicznych o sumarycznej pojemności większej od sumy pojemności dysków fizycznych zainstalowanych w macierzy. 5) Macierz musi obsługiwać do 2048 użytkowników lokalnych. |
| **Konfiguracja, zarządzanie**  | 1) Komunikacja z wbudowanym oprogramowaniem zarządzającym macierzą musi być możliwa w trybie graficznym np. poprzez przeglądarkę WWW.2) Musi być możliwe zdalne zarządzanie macierzą bez konieczności instalacji żadnych dodatkowych aplikacji na stacji administratora. |

**3.3. Dostawa dodatkowych dysków – 2 szt.**

|  |  |
| --- | --- |
| **Parametr lub warunek** | **Minimalne wymagania techniczne i funkcjonalne dla macierzy dyskowej** |
| **Pojemność** | 480 GB **Mixed-Us** |
| **Interfejs** | SATA 6.0 Gbps |
| **Format** | 2,5” |
| **Typ** | SSD |

1. **Usługi wdrożeniowe w zakresie konfiguracji urządzeń sieci LAN oraz Firewall**
	1. **Usługi rekonfiguracji sieci LAN (przełączniki, router) – 1 kpl.**

Przed przystąpieniem do prac wdrożeniowych związanych z konfiguracja urządzeń aktywnych sieci LAN - przełącznik CISCO Catalyst 2960-s wymagane jest opracowanie koncepcji technicznej obejmującej zakres wymaganych i sugerowanych do wdrożenia mechanizmów i technologii sieciowych.

Zakres prac instalacyjno-wdrożeniowych powinien obejmować co najmniej:

* + wykonanie segmentacji sieci (serwery, peryferia, stacje robocze) w oparciu o technologię 802.1Q.
	+ konfiguracje portów na przełącznikach w standardzie 802.1x – zezwalamy na dostęp do sieci tylko autoryzowanym użytkownikom
	+ konfigurację mechanizmów STP
	+ dodatkowo w celu ograniczenia niepożądanego ruchu w warstwie 2 wskazana jest izolacja poszczególnych komputerów (port isolation)
	1. **Usługi rekonfiguracji Firewall – 1 kpl.**

Przed rozpoczęciem prac wdrożeniowych, związanych z rekonfiguracją posiadanego przez Zamawiającego urządzenia bezpieczeństwa sieciowego firewall Fortigate 40F należy opracować ogólne założenia polityki bezpieczeństwa oraz koncepcję techniczną, która powinna zostać zatwierdzona przez Zamawiającego.

Zakres prac wdrożeniowych powinien obejmować co najmniej:

* Przygotowanie polityki bezpieczeństwa komunikacji z Internetem,
* Aktualizacja oprogramowania urządzeń do najnowszej wersji stabilnej, zalecanej przez producenta,
* Konfiguracja środowiska zarządzania w szczególności: ustawienie wszystkich parametrów związanych z adresacją i routingiem IP, ograniczenie zdalnego dostępu do urządzeń, konfiguracja autentykacji użytkowników, zapewnienie możliwości zarządzania poprzez protokoły SSH i HTTPS,
* Konfiguracja reguł zabezpieczeń komunikacji pomiędzy sieciami zgodnie z polityką bezpieczeństwa, ze szczególnym naciskiem konfiguracji listy aplikacji i stron WWW dopuszczonych i zabronionych dla użytkowników,
* Konfiguracja autentykacji użytkowników w zakresie dostępu do poszczególnych usług (aplikacji) w oparciu o usługi katalogowe AD
* Konfiguracja analizy ruchu SSL na poziomie protokołów HTTPS oraz SSH,
* Konfiguracja inspekcji ruchu pod katem programów złośliwych, wirusów itp.,
* Konfiguracja mechanizmów zabezpieczających przed znanymi atakami w sieci typu DoS, Spoofing, Sniffing itp.,
* Konfiguracja systemu raportowania oraz rejestru zdarzeń,
* Testy poprawności konfiguracji,
* Przygotowanie instrukcji wykonywania kopii konfiguracji urządzenia i odtwarzania w przypadku awarii,

**III. WARUNKI URUCHOMIENIA I ODBIORU WDROŻONYCH ROZWIĄZAŃ ORAZ PRZEKAZANIA DO EKSPLOATACJI**

* 1. **Pozostałe wymagania od Wykonawców**

Poza dostawami i usługami podstawowymi, wykonawca jest zobowiązany do skalkulowania wszelkich usług pomocniczych, jakie uzna za niezbędne do prawidłowego wykonania przedmiotu zamówienia dla przyjętej technologii, uwzględniając warunki ich wykonania.

Wykonawca musi ponadto uwzględnić w cenie w ramach kosztów dodatkowych –

* koszty dostawy sprzętu na miejsce instalacji
* koszty zabezpieczenia istniejących elementów obiektuoraz wyposażenia (urządzeń) Użytkownika przed ich zniszczeniem w trakcie wykonywania prac,
* koszty związane z zorganizowaniem pracy w sposób minimalizujący zakłócenie prowadzenia bieżącej działalności Zamawiającego
* koszty zapewnienia bezpieczeństwa bhp i ppoż. w trakcie realizacji prac
* koszty testów, prób, badań, odbiorów technicznych – jeśli będą wymagane

**Uwaga!**

Podmioty realizujące zadania publiczne zobowiązane są do stosowania rozwiązań z zakresu interoperacyjności mi. na poziomie technologicznym. Interoperacyjność osiąga się poprzez stosowania minimalnych wymagań dla systemów teleinformatycznych. Zgodnie z §20 ust. 2 pkt. 12 Rozporządzenia Rady Ministrów w sprawie Krajowych Ram Interoperacyjności (KRI) zapewnienie odpowiedniego poziomu bezpieczeństwa w systemach teleinformatycznych polega mi. na:

- zgodności systemów teleinformatycznych z odpowiednimi normami i politykami bezpieczeństwa

- redukcji ryzyk wynikających z wykorzystania opublikowanych podatności technicznych systemów teleinformatycznych

- zapewnienia bezpieczeństwa plików

- dbałość o aktualizację oprogramowania

Dodatkowym ważnym elementem systemu jest możliwość rejestrowania i przechowywania zapisów w dziennikach systemowych (logowanie zdarzeń).

Konieczność zapewnienia tej funkcjonalności wynika z:

1. §21 ust. 1 KRI (zapewnienie rozliczalności w systemach teleinformatycznych w postaci elektronicznej)
2. Art. 22 i 23 Ustawy z dnia 5 lipca 2018 o Krajowym Systemie Cyberbezpieczeństwa

Wdrożone rozwiązania powinny spełniając wymagania przywołanych aktów prawnych oraz standardów rynkowych.

* 1. **Przeszkolenie dla przedstawicieli**

 W ramach przedmiotu zamówienia wymagane jest przeprowadzenie szkolenia dla wyznaczonych pracowników Zamawiającego w zakresie:

* Archiwizacji danych oraz wykonywania kopi zapasowych
	1. **Dokumenty odbioru końcowego**
* Protokoły odbiorów częściowych
* Protokoły z pomiarów i testów – jeśli dotyczy
* Odpowiednie atesty i certyfikaty - jeśli są wymagane
* Instrukcje obsługi, dokumentacje i inne dokumenty dostarczane wraz ze sprzętem, przez producenta