Gmina Moszczenica
ul. Kosowska 1
97-310 Moszczenica
tel.: 44 616 96 25
fax: 44 616 96 87
e-mail: ug@moszczenica.pl
Oficjalna strona internetowa: http://www.moszczenica.pl/
BIP: http://bip.moszczenica.eu/
NIP: 771-16-61-550
REGON: 590647948

Moszczenica 29.07.2019 r.

INW.271. 29.2019

**Do Zainteresowanych**

***Dotyczy przetargu nieograniczonego o wartości szacunkowej zamówienia poniżej 221 000 euro na Dostawę sprzętu komputerowego i pomocy dydaktycznych dla szkół z terenu gminy Moszczenica.***

Na podst. art. 38 ust. 4 ustawy Prawo Zamówień Publicznych (t.j. Dz. U. z 2018 r. poz. 1986) Zamawiający informuje o modyfikacji treści załącznika nr 7 do SIWZ - Szczegółowej specyfikacji technicznej w zakresie opisów technicznych dot.:

1) laptopów - zapisy w ust. I pkt.1, ust. II pkt. 3, ust. III pkt. 1, ust. IV pkt. 4, ust. V pkt. 1, ust. VI pkt. 1 - w kolumnie *„Wymagane minimalne parametry techniczne":*

**Oprogramowanie zabezpieczające:**

1. System chroniący przed zagrożeniami, posiadający certyfikaty VB100%, OPSWAT, AVLAB +++, AV Comperative Advance +.
2. Musi umożliwiać co najmniej:
   - wykrywanie i blokowania plików ze szkodliwą zawartością, w tym osadzonych/skompresowanych plików, które używają czasie rzeczywistym algorytmów kompresji,
   - wykrywanie i usuwanie plików typu rootkit oraz złośliwego oprogramowania, również przy użyciu technik behawioralnych,
   - stosowanie kwarantanny,
   - wykrywanie i usuwanie fałszywego oprogramowania bezpieczeństwa (roguewear)
   - skanowanie urządzeń USB natychmiast po podłączeniu,
   - automatyczne odłączanie zainfekowanej końcówki od sieci,
   - skanowanie plików w czasie rzeczywistym, na żądanie, w interwałach czasowych lub poprzez harmonogram;
   - zbieranie informacji co najmniej o:
     - nazwie komputera,
     - producencie i modelu komputera,
     - przynależności do grupy roboczej/domeny,
     - szczegółach systemu operacyjnego,
     - lokalnych kontach użytkowników,
     - dacie i godzinie uruchomienia i ostatniego restartu komputera,
     - parametrach sprzętowych takich jak: procesor,RAM, numer seryjny, dysk, BIOS, interfejsach sieciowych, dołączonych urządzeniach peryferyjnych;
3. Moduł ochrony IDS/IPS
4. Mechanizm wykrywania skanowania portów
5. Musi pozwalać na wykluczenie adresów IP oraz PORTów TCP/IP z modułu wykrywania skanowania portów

6. Wykrywanie ataków DDoS;
7. Oprogramowanie do szyfrowania, chroniące dane na dysku, za pomocą algorytmów szyfrowania takich jak: AES, RC6, SERPENT i DWAFISH.
8. Pełne szyfrowanie dysków;
9. Szyfrowanie zawartości na urządzeń przenośnych, takich jak pendrive, dyski USB i udostępnianieich zawartości tylko autoryzowanym użytkownikom;
10. Centralna konsola zarządzająca musi umożliwiać co najmniej:
    - Przechowywanie danych w bazie typu SQL;
    - Zdalną instalację lub deinstalację oprogramowania na na pojedynczych komputerach, zakresie adresów IP lub grupie z domeny;
    - Tworzenie paczek instalacyjnych oprogramowania, z rozróżnieniem docelowej platformy systemowej (w tym 32 lub 64bit), w formie plików .exe, .msi oraz formatach dla systemów Linux;
    - Centralną dystrybucję uaktualnień definicji wirusów bez dostępu do sieci Internet.
    - Raportowanie przez dedykowany panel w konsoli z:
      - prezentacją tabelaryczną i graficzną;
      - możliwością automatycznego czyszczenia starych raportów;
      - możliwością eksportu do formatów CSV i PDF,
      - prezentujące dane zarówno z logowania zdarzeń konsoli, jak i dane/raporty zbierane ze stacji klienckich, w tym raporty o oprogramowaniu zainstalowanym na stacjach klienckich
11. Definiowanie struktury zarządzania opartej o role i polityki;
12. Wyświetlania statusu bezpieczeństwa urządzeń końcowych zainstalowanych w różnych lokalizacjach;
13. Tworzenie kopii zapasowych i przywracania plików konfiguracyjnych z chmury
14. Dostęp do konsoli z dowolnego miejsca;
15. Przeglądanie raportów podsumowujących dla wszystkich urządzeń;
16. Aktualizacja oprogramowania w trybie offline, za pomocą paczek aktualizacyjnych ściągniętych z dedykowanej witryny producenta oprogramowania;
17. Centralnie zarządzany z konsol, co najmniej w następującym zakresie:
    - różne ustawienia dostępu dla urządzeń: pełny dostęp, tylko do odczytu i blokowanie;
    - przyznwanie praw dostępu dla nośników pamięci USB, CD
    - regulowania połączeń WiFi i Bluetooth
    - kontrolowanie i regulowanie użycia urządzeń peryferyjnych typu: drukarki, skanery i kamery internetowe
    - blokada lub zezwolenia na połączenie z urządzeniami mobilnymi
    - możliwość tymczasowego dodania dostępu do urządzenia przez administratora;
    - szyfrowanie zawartości USB i udostępnianie jej na punktach końcowych z zainstalowanym oprogramowaniem zabezpieczającym;
    - możliwość zablokowania funkcjonalności portów USB, blokując dostęp urządzeniom innym niż klawiatura i myszka
    - możliwość zezwalania na dostęp tylko urządzeniom wcześniej dodanym przez administratora\
    - możliwość używania tylko zaufanych urządzeń sieciowych
18. Funkcja wirtualnej klawiatury
19. Możliwość blokowania każdej aplikacji
20. Możliwość zablokowania aplikacji w oparciu o kategorie
21. Możliwość dodania własnych aplikacji do listy zablokowanych
22. Tworzenie kompletnej listy aplikacji zainstalowanych na komputerach klientach poprzez konsole administracyjną;
23. Kategorie aplikacji minimum:
    a) tuning software,
    b) toolbars,
    c) proxy,
    d) network tools,
    e) file sharing application,
    f) backup software,
    g) encrypting tool
24. Generowanie i wysyłania raportów o aktywności na różnych kanałach transmisji danych, takich jak wymienne urządzenia, udziały sieciowe czy schowki;
25. Możliwość zablokowania funkcji Printscreen
26. Monitorowanie przesyłu danych między aplikacjami;

27. Blokowanie plików w oparciu o ich rozszerzenie lub rodzaj;
28. Ochrona przed wyciekiem informacji na drukarki lokalne i sieciowe;
29. Możliwość dodawania wyjątków dla domen, aplikacji i lokalizacji sieciowych
30. Ochrona plików zamkniętych w archiwach
31. Możliwość tworzenia profilu DLP dla każdej polityki
32. Wyświetlanie alertu dla użytkownika w chwili próby wykonania niepożądanego działania
33. Ochrona przez wyciekiem plików poprzez programy typu p2p
34. Możliwość monitorowania działań związanych z obsługą plików, takich jak kopiowanie, usuwanie, przenoszenie na dyskach lokalnych, dyskach wymiennych i sieciowych.
35. Monitorowania określonych rodzajów plików.
36. Możliwość wykluczenia określonych plików/folderów dla procedury monitorowania.
37. Raportowanie monitorowania zmian w plikach.
38. Możliwość śledzenia zmian we wszystkich plikach
39. Możliwość śledzenia zmian w zainstalowanym oprogramowaniu;
40. Usuwanie tymczasowych plików, czyszczenie niepotrzebnych wpisów do rejestru oraz defragmentacja dysku;
41. Możliwość zaplanowania optymalizacji na wskazanych stacjach klienckich

Zamawiający dysponuje obecnie 414 licencjami Kaspersky Lab, który został uruchomiony w całej infrastrukturze Zamawiającego tj. m.in. w Urzędzie Gminy oraz jednostkach organizacyjnych. Zamawiający wdrożył oprogramowanie Kaspersky Security Center w ramach którego nadzoruje funkcjonowanie wszystkich stacji roboczych. Zamawiający żąda dostawy oprogramowania klienckiego równoważnego, które będzie można nadzorować z poziomu jednej konsoli centralnej (administracyjnej). W przypadku dostawy oprogramowania równoważnego do Kaspersky dostawca ma obowiązek dostawy, instalacji i konfiguracji oprogramowania do zarządzania stajami klienckimi wraz instalacją niezbędnego oprogramowania na stacjach klienckich oraz instalacji systemu operacyjnego na maszynie wirtualnej w infrastrukturze Zamawiającego służącej do zarządzania nowo dostarczonym antywirusem na stacjach klienckich.

Licencja na dostarczone oprogramowanie musi posiadać możliwość aktualizowania baz wirusów, itp. na okres conajmniej 5 lat. Dostarczone oprogramowanie nie może być gorsze w rankingu AV-TEST, AV-Comparatives niż Kaspersky Lab.

**System operacyjny:**

System operacyjny klasy PC musi spełniać następujące wymagania poprzez wbudowane mechanizmy, bez użycia dodatkowych aplikacji:

1. Dostępne dwa rodzaje graficznego interfejsu użytkownika:
   a) Klasyczny, umożliwiający obsługę przy pomocy klawiatury i myszy,
   b) Dotykowy umożliwiający sterowanie dotykiem na urządzeniach typu tablet lub monitorach dotykowych
2. Funkcje związane z obsługą komputerów typu tablet, z wbudowanym modułem „uczenia się" pisma użytkownika – obsługa języka polskiego
3. Interfejs użytkownika dostępny w języku polskim i angielskim
4. Możliwość tworzenia pulpitów wirtualnych, przenoszenia aplikacji pomiędzy pulpitami i przełączanie się pomiędzy pulpitami za pomocą skrótów klawiaturowych lub GUI.
5. Wbudowane w system operacyjny minimum dwie przeglądarki Internetowe
6. Zintegrowany z systemem moduł wyszukiwania informacji (plików różnego typu, tekstów, metadanych) dostępny z poziomów: menu, otwartego okna systemu operacyjnego;
7. System wyszukiwania oparty na konfigurowalnym przez użytkownika module indeksacji zasobów lokalnych,
8. Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, pomoc, komunikaty systemowe, menedżer plików.
9. Graficzne środowisko instalacji i konfiguracji w języku polskim
10. Wbudowany system pomocy w języku polskim.
11. Możliwość przystosowania stanowiska dla osób niepełnosprawnych (np. słabo widzących).

12. Możliwość dokonywania aktualizacji i poprawek systemu poprzez mechanizm zarządzany przez administratora Zamawiającego.
13. Możliwość dostarczania poprawek do systemu operacyjnego w modelu peer-to-peer.
14. Możliwość sterowania czasem dostarczania nowych wersji systemu operacyjnego, w tym możliwość centralnego opóźniania dostarczania nowej wersji o minimum 4 miesiące.
15. Zabezpieczony hasłem hierarchiczny dostęp do systemu;
16. Konta i profile użytkowników zarządzane zdalnie;
17. Praca systemu w trybie ochrony kont użytkowników.
18. Możliwość dołączenia systemu do usługi katalogowej on-premise lub w chmurze;
19. Molliwość zablokowania urządzenia w ramach danego konta tylko do uruchamiania wybranej aplikacji - tryb "kiosk".
20. Możliwość automatycznej synchronizacji plików i folderów roboczych znajdujących się na serwerze plików z prywatnym urządzeniem, bez konieczności łączenia się z siecią VPN z poziomu folderu użytkownika
21. Zdalna pomoc i współdzielenie aplikacji – możliwość zdalnego przejęcia sesji zalogowanego użytkownika celem rozwiązania problemu z komputerem.
22. Transakcyjny system plików pozwalający na stosowanie przydziałów (ang. quota) na dysku dla użytkowników oraz zapewniający większą niezawodność i pozwalający tworzyć kopie zapasowe.
23. Oprogramowanie dla tworzenia kopii zapasowych (Backup);
24. Automatyczne wykonywanie kopii plików z możliwością automatycznego przywrócenia wersji wcześniejszej.
25. Możliwość przywracania obrazu plików systemowych do uprzednio zapisanej postaci.
26. Możliwość przywracania systemu operacyjnego do stanu początkowego z pozostawieniem plików użytkownika.
27. Możliwość blokowania lub dopuszczania dowolnych urządzeń peryferyjnych za pomocą polityk grupowych (np. przy użyciu numerów identyfikacyjnych sprzętu);
28. Wbudowany mechanizm wirtualizacji typu hypervisor;
29. Wbudowana możliwość zdalnego dostępu do systemu i pracy zdalnej z wykorzystaniem interfejsu graficznego.
30. Bezpłatne biuletyny bezpieczeństwa związane z działaniem systemu operacyjnego.
31. Wbudowana zapora internetowa (firewall) dla ochrony połączeń internetowych;
32. Zintegrowana z systemem konsola do zarządzania ustawieniami zapory i regułami IP v4 i v6.
33. Identyfikacja sieci komputerowych, do których jest podłączony system operacyjny;
34. Zapamiętywanie ustawień i przypisywanie do min. 3 kategorii bezpieczeństwa z predefiniowanymi odpowiednio do kategorii ustawieniami zapory sieciowej i udostępnianiem plików;
35. Możliwość zdefiniowania zarządzanych aplikacji w taki sposób aby automatycznie szyfrowały pliki na poziomie systemu plików.
36. Blokowanie bezpośredniego kopiowania treści między aplikacjami zarządzanymi i niezarządzanymi.
37. Wbudowany system uwierzytelnienia dwuskładnikowego oparty o certyfikat lub klucz prywatny oraz PIN lub uwierzytelnienie biometryczne;
38. Wbudowany system szyfrowania dysku twardego ze wsparciem modułu TPM
39. Możliwość tworzenia i przechowywania kopii zapasowych kluczy odzyskiwania do szyfrowania dysku w usługach katalogowych;
40. Możliwość tworzenia wirtualnych kart inteligentnych.

41. Wsparcie dla firmware UEFI i funkcji bezpiecznego rozruchu (Secure Boot)
42. Wsparcie dla IPSEC oparte na politykach;
43. Wdrażanie IPSEC oparte na zestawach reguł definiujących ustawienia zarządzanych w sposób centralny;
44. Mechanizmy logowania w oparciu o:
    a) Login i hasło,
    b) Karty inteligentne i certyfikaty (smartcard),
    c) Wirtualne karty inteligentne i certyfikaty chronione poprzez moduł TPM;umozliwiajacy pracę w domenie;

Zamawiający dysponuje rozległą siecią komputerową do której podłączone są wszystkie jego jednostki organizacyjne w tym szkoły objęte przedmiotowym projektem. Zarządzanie bezpieczeństwem całej sieci, w tym dostępem do zasobów odbywa się na bazie serwerów Windows Server i m.in. wdrożonej na nich usłudze Active Directory. Zamawiający w świetle prawa jest operatorem telekomunikacyjnymi wpisanym w UKE do rejestru JST. Zatem ciążą na nim m.in. obowiązki związane z logowaniem ruchu sieciowego. Obecnie obowiązek ten realizowany jest m.in. przy pomocy dwóch urządzeń firewall PaloAlto pracujących trybie Active Active, które integrują się z usługą Active Directory i wykazem istniejących tam kont użytkowników oraz grup użytkowników. Na tej podstawie tworzone są reguły bezpieczeństwa sieci i monitorowany jest ruch sieciowy. Zmawiający żąda, aby dostarczony sprzęt komputerowy został wyposażony w system operacyjny, który w pełni będzie integrował się z istniejącą usługą Active Directory, w tym GPO (m.in. automatyzacja procesów instalacji oprogramowania). Wykonawca ma obowiązek dostarczyć sprzęt z systemem operacyjnym, wraz z odpowiednią ilością licencji CAL. Dostarczone oprogramowanie musi być w najnowszej dostępnej wersji.

Zmienia się na:

**Oprogramowanie zabezpieczające:**

Zamawiający dysponuje obecnie 414 licencjami Kaspersky Lab, który został uruchomiony w całej infrastrukturze Zamawiającego tj. m.in. w Urzędzie Gminy oraz jednostkach organizacyjnych. Zamawiający wdrożył oprogramowanie Kaspersky Security Center w ramach którego nadzoruje funkcjonowanie wszystkich stacji roboczych. Zamawiający żąda dostawy oprogramowania klienckiego równoważnego, które będzie można nadzorować z poziomu jednej konsoli centralnej (administracyjnej). W przypadku dostawy oprogramowania równoważnego do Kaspersky dostawca ma obowiązek dostawy, instalacji i konfiguracji oprogramowania do zarządzania stajami klienckimi wraz instalacją niezbędnego oprogramowania na stacjach klienckich oraz instalacji systemu operacyjnego na maszynie wirtualnej w infrastrukturze Zamawiającego służącej do zarządzania nowo dostarczonym antywirusem na stacjach klienckich.
Licencja na dostarczone oprogramowanie musi posiadać możliwość aktualizowania baz wirusów, itp. na okres conajmniej 5 lat. Dostarczone oprogramowanie nie może być gorsze w rankingu AV-TEST, AV-Comparatives niż Kaspersky Lab.

**System operacyjny:**

Zamawiający dysponuje rozległą siecią komputerową do której podłączone są wszystkie jego jednostki organizacyjne w tym szkoły objęte przedmiotowym projektem. Zarządzanie bezpieczeństwem całej sieci, w tym dostępem do zasobów odbywa się na bazie serwerów Windows Server i m.in. wdrożonej na nich usłudze Active Directory. Zamawiający w świetle prawa jest operatorem telekomunikacyjnymi wpisanym w UKE do rejestru JST. Zatem ciążą na nim m.in. obowiązki związane z logowaniem ruchu sieciowego. Obecnie obowiązek ten realizowany jest m.in. przy pomocy dwóch urządzeń firewall PaloAlto pracujących trybie Active Active, które integrują się z usługą Active Directory i wykazem istniejących tam kont użytkowników oraz grup użytkowników. Na tej podstawie tworzone są reguły bezpieczeństwa sieci i monitorowany jest ruch sieciowy. Zmawiający żąda, aby dostarczony sprzęt komputerowy został wyposażony w system operacyjny, który w pełni będzie integrował się z istniejącą usługą Active Directory, w tym GPO (m.in.

automatyzacja procesów instalacji oprogramowania). Wykonawca ma obowiązek dostarczyć sprzęt z systemem operacyjnym, wraz z odpowiednią ilością licencji CAL. Dostarczone oprogramowanie musi być w najnowszej dostępnej wersji.
System operacyjny powinien również oferować ułatwienia dostępu dla osób niepełnosprawnych (np.: narracja, lupa, duży kontrast)

2) tabletów - zapisy w ust. I pkt. 2, ust. II pkt. 2, ust. III pkt 5, ust. V pkt. 9 - w kolumnie *„Wymagane minimalne parametry techniczne":*

**Oprogramowanie zabezpieczające:**

1. Oprogramowanie musi pozwalać na pełne oraz szybkie skanowanie
2. Stałe skanowanie w tle
3. Skanowanie w celu wykrycia zagrożeń typu malware
4. Skanowanie karty pamięci
5. Wyznaczenie wyjątków od skanowania na poziomie plików i folderów.
6. Analizowanie pod kątem luk w bezpieczeństwie oraz raportowanie o wystąpieniu o takiej sytuacji.
7. Harmonogram skanowania musi mieć możliwość uruchomienia skanowania w chwili wykrycia że urządzenie jest ładowane
8. Analizowanie ustawień urządzenia w celu minimalizowania zagrożeń oraz przekierowywanie do ustawień które powinny być zamienione.
9. Analizowanie ustawienia następujących funkcji
   - o Konta i synchronizacja
   - o Bluetooth
   - o Szyfrowanie pamięci urządzenia
   - o Blokada ekranu
   - o Nieznane źródła aplikacji
   - o Debugowanie USB
   - o Wi-Fi
10. Monitorowanie dostepu aplikacji do:
    - o Kontaktów
    - o Danych identyfikacyjnych
    - o Śledzenia lokalizacji
    - o Wiadomości
    - o Internetu
11. Ochrona przeglądania Internetu
12. Ochrona przed atakami typu Phishing.
13. Analizowanie uruchomionych aplikacji i zamykanie nieużywanych;
14. Kontrola jasności ekranu, kontrola WiFi i bluetooth.
15. Tworzenie raportów wykorzystania CPU, żywotności baterii oraz pamięci;
16. Funkcjonalność białej listy aplikacji które nie są zatrzymywane.
17. Monitorowanie wykorzystania sieci;
18. Informowanie o zbliżającym się limicie danych oraz blokowanie w przypadku jego osiągnięcia;
19. Wykonywanie kopii zapasowej w chmurze I jej odzyskiwanie;
20. Bezpieczne usuwanie danych z urządzenia i wszystkich jego nośników.
21. Ochrona rodzicielska która to umozliwia co najmniej:
    - o Blokowania stron po kategoriach , w tym co najmniej: oprogramowanie, media społecznościowe, tylko dla dorosłych;
    - o Blokowanie stron z wyszczególnionego adresu URL co najmniej dla: dla Chrome, Firefox, Maxthon, Opera i Dolphin;
    - o Ustawiania wyjątków adresów URL
22. Moduł, w którym producent udostepnia informację o nowych aktualizacjach i ważnych alarmach bezpieczeństwa.
23. Raporty:
    - o Znalezione wirusy
    - o Aktywności związane z ochroną przed kradzieżą
    - o Strony internetowe które zostały zablokowane
    - o Informacje o kopi zapasowej

- o Informacje o ostatniej aktualizacji bazy wirusów

24. Zdalne pobieranie lokalizacji urządzenia
25. Zdalne usuwanie danych w przypadku kradzieży urządzenia;
26. Oprogramowanie musi udostępniać kamerę i mikrofon w celu rejestracji obrazu i dźwięku, w przypadku kradzieży urządzenia.
27. Informowanie o poziomie bezpieczeństwa urządzenia, w graficzny sposób.
28. Automatyczne aktualizacje;
29. W przypadku dwóch nieudanych prób wprowadzenia hasła blokady ekranu, automatyczne wykonywanie zdjęcia przy wykorzystaniu aparatu na froncie i tyle urządzenia;
30. Skróty do ustawień WiFI, Bluethoot, przesyłania danych pakietowych.
31. Certyfikaty AVTest oraz AV Comparatives Approved mobile produkt.
32. Konto w chmurze o pojemności 1GB
33. W przypadku zgubienia kodu PIN, możliwość uwierzytelnienia się przez zaufane konto w chmurze przez wifi;
34. Wsparcie dostępne przez chat oraz www.
35. Możliwość okreslenia do jakich danych prywatnych może mogą mieć dostęp aplikacje producentów trzecich;
36. Możliwość sprawdzenia zużycia pamięci RAM w danym czasie;
37. Możliwość wyłączenia działających w tle aplikacji;
38. Śledzenie zużycie baterii;
39. Blokowanie kodem PIN dostępu do kontaktów aplikacji, dokumentów galerii zdjęć i video, z możliwością wyboru pojedynczego element z tej listy;

Zamawiający dysponuje obecnie 414 licencjami Kaspersky Lab, który został uruchomiony w całej infrastrukturze Zamawiającego tj. m.in. w Urzędzie Gminy oraz jednostkach organizacyjnych. Zamawiający wdrożył oprogramowanie Kaspersky Security Center w ramach którego nadzoruje funkcjonowanie wszystkich stacji roboczych. Zamawiający żąda dostawy oprogramowania klienckiego równoważnego, które będzie można nadzorować z poziomu jednej konsoli centralnej (administracyjnej). W przypadku dostawy oprogramowania równoważnego do Kaspersky dostawca ma obowiązek dostawy, instalacji i konfiguracji oprogramowania do zarządzania stajami klienckimi wraz instalacją niezbędnego oprogramowania na stacjach klienckich oraz instalacji systemu operacyjnego na maszynie wirtualnej w infrastrukturze Zamawiającego służącej do zarządzania nowo dostarczonym antywirusem na stacjach klienckich.

Licencja na dostarczone oprogramowanie musi posiadać możliwość aktualizowania baz wirusów, itp. na okres conajmniej 5 lat. Dostarczone oprogramowanie nie może być gorsze w rankingu AV-TEST, AV-Comparatives niż Kaspersky Lab.

## System operacyjny:

Musi umożliwiać:

1. Komunikację głosową z aplikacjami obsługującymi usługę interakcji głosowej.
2. Bezpośrednie udostępnianie materiałów wybranym osobom w wybranych aplikacjach.
3. Uśpienie urządzenia.
4. Przełączenie aplikacji rzadziej używanych w tryb czuwania co zmniejsza zużycie baterii.
5. Obsługę USB oraz ładowanie urządzenia i przesyłanie danych z użyciem tego samego kabla.
6. Sterowanie uprawnieniami zainstalowanych aplikacji.
7. Weryfikację przy uruchomieniu czy oprogramowanie układowe lub system operacyjny różni się od wersji fabrycznej.
8. Obsługę rysika Bluetooth w tym klawiszy modyfikujących oraz czułości na nacisk.
9. Zaznaczanie tekstu.
10. Cofanie/przywracanie oraz inne działania na tekście.
11. Tłumaczenie tekstu.
12. Drukowanie dwustronne.
13. Automatyczną obsługę internetowych adresów URL zainstalowanych aplikacji, co musi pozwalać na ich uruchamianie zamiast ich stron internetowych.
14. Zarządzanie głośnością powiadomień, muzyki i alarmów.
15. Działanie jako przenośny hotspot Wi-Fi z obsługą pasma 5 GHz.
16. Używanie kart microSD i pamięci zewnętrznych jako zaszyfrowanej, rozszerzonej pamięci.
17. Przenoszenie konta, aplikacji i danych na nowe urządzenie.
18. Tworzenie automatycznej kopii zapasowej aplikacji.
19. Tworzenie i przywracanie kopii zapasowej dodatkowych ustawień systemu, takich jak ustawienia synchronizacji, preferowane aplikacje, ustawienia ułatwień dostępu

Zamawiający dysponuje rozległą siecią komputerową do której podłączone są wszystkie jego jednostki organizacyjne w tym szkoły objęte przedmiotowym projektem. Zarządzanie bezpieczeństwem całej sieci, w tym dostępem do zasobów odbywa się na bazie serwerów Windows Server i m.in. wdrożonej na nich usłudze Active Directory. Zamawiający w świetle prawa jest operatorem telekomunikacyjnymi wpisanym w UKE do rejestru JST. Zatem ciążą na nim m.in. obowiązki związane z logowaniem ruchu sieciowego. Obecnie obowiązek ten realizowany jest m.in. przy pomocy dwóch urządzeń firewall PaloAlto pracujących trybie Active Active, które integrują się z usługą Active Directory i wykazem istniejących tam kont użytkowników oraz grup użytkowników. Na tej podstawie tworzone są reguły bezpieczeństwa sieci i monitorowany jest ruch sieciowy. Zmawiający żąda, aby dostarczony sprzęt komputerowy został wyposażony w system operacyjny, który w pełni będzie integrował się z istniejącą usługą Active Directory, w tym GPO (m.in. automatyzacja procesów instalacji oprogramowania). Wykonawca ma obowiązek dostarczyć sprzęt z systemem operacyjnym, wraz z odpowiednią ilością licencji CAL. Dostarczone oprogramowanie musi być w najnowszej dostępnej wersji.

Zmienia się na:

**Oprogramowanie zabezpieczające:**

Zamawiający dysponuje obecnie 414 licencjami Kaspersky Lab, który został uruchomiony w całej infrastrukturze Zamawiającego tj. m.in. w Urzędzie Gminy oraz jednostkach organizacyjnych. Zamawiający wdrożył oprogramowanie Kaspersky Security Center w ramach którego nadzoruje funkcjonowanie wszystkich stacji roboczych. Zamawiający żąda dostawy oprogramowania klienckiego równoważnego, które będzie można nadzorować z poziomu jednej konsoli centralnej (administracyjnej). W przypadku dostawy oprogramowania równoważnego do Kaspersky dostawca ma obowiązek dostawy, instalacji i konfiguracji oprogramowania do zarządzania stajami klienckimi wraz instalacją niezbędnego oprogramowania na stacjach klienckich oraz instalacji systemu operacyjnego na maszynie wirtualnej w infrastrukturze Zamawiającego służącej do zarządzania nowo dostarczonym antywirusem na stacjach klienckich.
Licencja na dostarczone oprogramowanie musi posiadać możliwość aktualizowania baz wirusów, itp. na okres conajmniej 5 lat. Dostarczone oprogramowanie nie może być gorsze w rankingu AV-TEST, AV-Comparatives niż Kaspersky Lab.

**System operacyjny:**

Musi umożliwiać:

1. Komunikację głosową z aplikacjami obsługującymi usługę interakcji głosowej.
2. Bezpośrednie udostępnianie materiałów wybranym osobom w wybranych aplikacjach.
3. Uśpienie urządzenia.
4. Przełączenie aplikacji rzadziej używanych w tryb czuwania co zmniejsza zużycie baterii.
5. Obsługę USB oraz ładowanie urządzenia i przesyłanie danych z użyciem tego samego kabla.
6. Sterowanie uprawnieniami zainstalowanych aplikacji.
7. Weryfikację przy uruchomieniu czy oprogramowanie układowe lub system operacyjny różni się od wersji fabrycznej.
8. Obsługę rysika Bluetooth w tym klawiszy modyfikujących oraz czułości na nacisk.
9. Zaznaczanie tekstu.
10. Cofanie/przywracanie oraz inne działania na tekście.
11. Tłumaczenie tekstu.
12. Drukowanie dwustronne.
13. Automatyczną obsługę internetowych adresów URL zainstalowanych aplikacji, co

musi pozwalać na ich uruchamianie zamiast ich stron internetowych.

14. Zarządzanie głośnością powiadomień, muzyki i alarmów.
15. Działanie jako przenośny hotspot Wi-Fi z obsługą pasma 5 GHz.
16. Używanie kart microSD i pamięci zewnętrznych jako zaszyfrowanej, rozszerzonej pamięci.
17. Przenoszenie konta, aplikacji i danych na nowe urządzenie.
18. Tworzenie automatycznej kopii zapasowej aplikacji.
19. Tworzenie i przywracanie kopii zapasowej dodatkowych ustawień systemu, takich jak ustawienia synchronizacji, preferowane aplikacje, ustawienia ułatwień dostępu

W załączeniu do niniejszego pisma zamieszcza się zmodyfikowany załącznik nr 7 do SIWZ - Szczegółową specyfikację techniczną.

Z up. WOJTA GMINY
*Krzysztof Jędrzejczyk*
SEKRETARZ GMINY

Do wiadomości:

1. Adresat
2. a/a