Załącznik nr 9 do SWZ

OPIS PRZEDMIOTU ZAMÓWIENIA

Nazwa zadania: „Dostawa sprzętu komputerowego w ramach projektu ”Wsparcie dzieci z rodzin pegeerowskich w rozwoju cyfrowym – Granty PPGR””.

Inwestor: Gmina Łąck, ul. Gostynińska 2, 09-520 Łąck

Wspólny słownik zamówień (CPV):

30213100-6 – Komputery przenośne;

30213000-5 – Komputery osobiste;

48700000-5 – Pakiety oprogramowania użytkowego;

48310000-4 – Pakiety oprogramowania do tworzenia dokumentów;

48620000-0 – Systemy operacyjne.

I. Przedmiot zamówienia.

1. Przedmiot niniejszego zamówienia stanowi: „Dostawa sprzętu komputerowego w ramach projektu: „Wsparcie dzieci z rodzin pegeerowskich w rozwoju cyfrowym – Granty PPGR””.
2. Na realizację przedmiotowego zamówienia Zamawiający otrzymał dofinansowanie w ramach Programu Operacyjnego Polska Cyfrowa na lata 2014-2020, Osi Priorytetowej V Rozwój cyfrowy JST oraz wzmocnienie cyfrowej odporności na zagrożenia REACT-EU, działanie 5.1. Rozwój cyfrowy JST oraz wzmocnienie cyfrowej odporności na zagrożenia dotyczące realizacji projektu grantowego „Wsparcie dzieci z rodzin pegeerowskich w rozwoju cyfrowym – Granty PPGR”.
3. Przedmiot zamówienia obejmuje dostawę 90 sztuk laptopów, 4 sztuk tabletów oraz 94 sztuki oprogramowania.

II. Wymagane minimalne parametry.

1. Laptop

Lp.	Nazwa komponentu	Wymagane minimalne parametry techniczne komputerów
1.	Procesor	Procesor wielordzeniowy ze zintegrowaną grafiką, zaprojektowany do pracy w komputerach klasy x86, pamięć podręczna procesora 4MB L3, podstawowa częstotoliwość procesora 2,3GHz lub równoważny na poziomie wydajności liczonej w punktach na podstawie PerformanceTest w teście CPU Mark według wyników opublikowanych na http://www.cpubenchmark.net/. Wykonawca w składanej ofercie winien podać dokładny model oferowanego podzespołu.
2.	Pamięć operacyjna RAM	Min. 8 GB 2400MHz non-ECC 1 slot na pamięć umożliwiający wymianę kości RAM
3.	Parametry pamięci masowej	M.2 256GB SSD PCIe NVMe
4.	Karta graficzna	Zintegrowana z procesorem komputera
5.	Wyposażenie multimedialne	Karta dźwiękowa zintegrowana z płytą główną, zgodna z High Definition. Wbudowane w obudowie komputera: głośniki stereo (2x3W), port słuchawek i mikrofonu (dopuszcza się złącze typu COMBO),wbudowana kamera video 720p, oraz mikrofon cyfrowy.
6.	Napęd optyczny	brak
7.	Płyta główna	Płyta główna zaprojektowana i wyprodukowana na zlecenie producenta komputera, trwale oznaczona (na laminacie płyty głównej) na etapie produkcji nazwą producenta oferowanej jednostki i dedykowana dla danego urządzenia. Płyta główna wyposażona w BIOS producenta komputera, zawierający numer seryjny komputera oraz numer seryjny płyty głównej.
8.	Zgodność z systemami operacyjnymi	Oferowany model komputera musi poprawnie współpracować z zamawianym systemem operacyjnym (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).
9.	BIOS	BIOS zgodny ze specyfikacją UEFI, wyprodukowany przez producenta komputera, zawierający logo producenta komputera lub nazwę producenta komputera. Pełna obsługa BIOS za pomocą klawiatury i myszy. Możliwość, bez uruchamiania systemu operacyjnego z dysku twardego komputera, bez dodatkowego oprogramowania z zewnętrznych i podłączonych do niego urządzeń zewnętrznych odczytania z BIOS informacji o: - wersji BIOS wraz z datą produkcji BIOS - nr seryjnym komputera - Ilości zainstalowanej pamięci RAM - typie procesora i jego prędkości - MAC adresu zintegrowanej karty sieciowej - nr seryjnym płyty głównej komputera - informacja o licencji systemu operacyjnego, która została zaimplementowana w BIOS Administrator z poziomu BIOS musi mieć możliwość wykonania poniższych czynności: - Możliwość włączania/wyłączania wirtualizacji z poziomu BIOS

		- Możliwość ustawienia kolejności bootowania oraz wyłączenia poszczególnych urządzeń z listy startowej. - Funkcja bezpiecznego usuwania danych z dysku
10.	Ekran	Matowy, matryca 15,6” z podświetleniem w technologii LED Rozdzielczość FHD 1920x1080, Jasność min. 250nits, Matryca wykonana w technologii IPS z cienką ramką.
11.	Interfejsy / Komunikacja	3xUSB z czego min. 2xUSB-A port na boku obudowy o przepustowości 5Gb/s oraz 1 port Typu-C o przepustowości 5Gb/s , RJ-45, port słuchawek i mikrofonu (dopuszcza się złącze typu COMBO), czytnik karta pamięci SDXC, HDMI 1.4b, gniazdo zasilania sieciowego o mocy 45W
12.	Karta sieciowa LAN	RJ-45 – 10/100/1000
13.	Karta sieciowa WLAN	Wbudowana karta sieciowa, pracująca w standardzie 802.11 a/b/g/n/ac Bluetooth min. 4.0
14.	Klawiatura i mysz	Wbudowana w obudowie laptopa/notebooka, klawiatura z panelem klawiszy numerycznych, touch-pad z obsługą gestów.
15.	Zasilacz	Energooszczędny zasilacz o mocy max 45W
16.	Certyfikaty, oświadczenia i standardy	- Certyfikat środowiskowy EPEAT - ENERGY STAR - Deklaracja zgodności CE - Dla producenta sprzętu należy dostarczyć certyfikat ISO 9001, ISO 14001,
17.	Waga/Wymiary	Waga produktu nie może przekroczyć 1,74kg, minimalne wymiary obudowy głęb/wys/szer 24,2x1,99x35,8 cm
18.	System operacyjny	Microsoft Windows 10/11 64 bit
19.	Oprogramowanie do aktualizacji sterowników	Oprogramowanie producenta oferowanego sprzętu umożliwiające automatyczna weryfikacje i instalację sterowników. Oprogramowanie musi automatycznie łączyć się z centralna bazą sterowników i oprogramowania producenta, sprawdzać dostępne aktualizacje i zapewniać zbiorczą instalację wszystkich sterowników i aplikacji bez ingerencji użytkownika.
20.	Gwarancja	Minimalny czas trwania wsparcia technicznego producenta wynosi 24 miesiące. Firma serwisująca musi posiadać ISO 9001 na świadczenie usług serwisowych oraz posiadać autoryzacje producenta urządzeń
21.	Wsparcie techniczne producenta	– Zaawansowana diagnostyka sprzętowa oraz oprogramowania dostępna 24h/dobę na stronie producenta komputera. – Bezpośredni kontakt z Autoryzowanym Partnerem Serwisowym Producenta (brak konieczności zgłaszania każdej usterki sprzętowej telefonicznie), mający na celu przyśpieszenie procesu diagnostyki i skrócenia czasu usunięcia usterki. – Aktualna lista Autoryzowanych Partnerów Serwisowych dostępna na stronie Producenta komputera. – Infolinia wsparcia technicznego dedykowana do rozwiązywania usterek oprogramowania – możliwość kontaktu przez telefon, formularz web lub chat online, dostępna w dni powszednie od 8:00-16:00.

		– Wsparcie techniczne świadczone przez producenta lub autoryzowanego partnera serwisowego dla urządzeń i preinstalowanego oprogramowania OEM, zakupionego z urządzeniem, dostarczane zdalnie. – Możliwość sprawdzenia aktualnego okresu i poziomu wsparcia technicznego dla urządzeń za pośrednictwem strony internetowej producenta. – Możliwość sprawdzenia konfiguracji sprzętowej komputera oraz warunków gwarancji po podaniu numeru seryjnego bezpośrednio na stronie producenta.

2. Tablet

Lp.	Nazwa komponentu	Wymagane minimalne parametry techniczne komputerów
1.	Procesor	Procesor zaprojektowany do pracy w tabletach o częstotliwości nie mniejszej niż: 1,6GHz, lub równoważny Wykonawca w składanej ofercie winien podać dokładny model oferowanego podzespołu.
2.	Pamięć operacyjna RAM	Min. 4 GB
3.	Parametry pamięci masowej	Min. 64GB
4.	Wyposażenie multimedialne	Karta dźwiękowa zintegrowana z płytą główną, Wbudowane w obudowie: głośniki stereo, port słuchawek i mikrofonu ,wbudowana kamera video przód: min. 5Mpix, tył CMOS 8Mpix, oraz mikrofon cyfrowy, Slot karty micr, SD do 256GB, bluetooth min 5.0, karta Wi-Fi dwu zakresowa 802.11 a/b/g/n/ac oraz modem 4G 800/900/1800/2100/2600 MHz.
5.	Zgodność z systemami operacyjnymi	Oferowany system musi poprawnie współpracować z zamawianym systemem operacyjnym ANDROID w wersji min. 10-tej.
6.	Ekran	Min 10,1" pojemnościowy w technologii LED Rozdzielczość FHD 1920x1080, Matryca wykonana w technologii IPS
7.	Interfejsy / Komunikacja	1x USB typ C, 1 x slot kart micro SD, 1 x Jack
8.	Klawiatura i mysz	Bezprzewodowa dołączona do zestawu
9.	Zasilanie	Ładowarka 100-240V, dołączona do zestawu
10.	Akumulator	Min. 7000 mAh
11.	Wymiary	Max. 8mm x 163mm x 244mm
12.	Gwarancja	Minimalny czas trwania wsparcia technicznego producenta wynosi 24 miesiące.

3. Oprogramowanie antywirusowe

Szczegółowy opis
Administracja **zdalna** 1. Rozwiązanie musi wspierać instalację na systemach Windows Server (od 2012), Linux oraz w postaci maszyny wirtualnej w formacie OVA lub dysku wirtualnego w formacie VHD. 2. Rozwiązanie musi zapewniać instalację z użyciem nowego lub istniejącego serwera bazy danych MS SQL i MySQL. 3. Rozwiązanie musi zapewniać pobranie wszystkich wymaganych elementów serwera centralnej administracji w postaci jednego pakietu instalacyjnego i każdego z modułów oddzielnie bezpośrednio ze strony producenta. 4. Rozwiązanie musi zapewniać dostęp do konsoli centralnego zarządzania w języku polskim z poziomu interfejsu WWW

zabezpieczony za pośrednictwem protokołu SSL.
5. Rozwiązanie musi zapewniać zabezpieczoną komunikację pomiędzy poszczególnymi modułami serwera za pomocą certyfikatów.
6. Rozwiązanie musi zapewniać utworzenia własnego CA (Certification Authority) oraz dowolnej liczby certyfikatów z podziałem na typ elementu: agent, serwer zarządzający, serwer proxy, moduł zarządzania urządzeniami mobilnymi.
7. Rozwiązanie musi wspierać zarządzanie urządzeniami z systemem iOS i Android.
8. Rozwiązanie musi zapewniać centralną konfigurację i zarządzanie przynajmniej takimi modułami jak: ochrona antywirusowa, antyspyware, które działają na stacjach roboczych w sieci.
9. Rozwiązanie musi zapewniać weryfikację podzespołów zarządzanego komputera (w tym przynajmniej: producent, model, numer seryjny, informacje o systemie, procesor, pamięć RAM, wykorzystanie dysku twardego, informacje o wyświetlaczu, urządzenia peryferyjne, urządzenia audio, drukarki, karty sieciowe, urządzenia masowe).
10. Rozwiązanie musi zapewniać instalowanie i odinstalowywanie oprogramowania firm trzecich dla systemów Windows oraz MacOS oraz odinstalowywanie oprogramowania zabezpieczającego firm trzecich, zgodnych z technologią OPSWAT.
11. Rozwiązanie musi zapewniać wymuszenia dwufazowej autoryzacji podczas logowania do konsoli administracyjnej.
12. Serwer administracyjny musi posiadać możliwość tworzenia grup statycznych i dynamicznych komputerów.
13. 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.
14. Rozwiązanie musi zapewniać korzystanie z minimum 100 szablonów raportów, przygotowanych przez producenta oraz musi zapewniać tworzenie własnych raportów przez administratora.
15. Rozwiązanie musi zapewniać wysłanie powiadomienia przynajmniej za pośrednictwem wiadomości email, komunikatu SNMP oraz do dziennika syslog.
16. Rozwiązanie musi zapewniać podział uprawnień administratorów w taki sposób, aby każdy z nich miał możliwość zarządzania konkretnymi grupami komputerów, politykami oraz zadaniami.

Ochrona stacji roboczych

1. Rozwiązanie musi wspierać systemy operacyjne Windows (Windows 7/Windows 8/Windows 8.1/Windows 10/Windows 11).
2. Rozwiązanie musi wspierać architekturę ARM64.
3. Rozwiązanie musi zapewniać wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor.
4. Rozwiązanie musi posiadać wbudowaną technologię do ochrony przed rootkitami oraz podłączeniem komputera do sieci botnet.
5. Rozwiązanie musi zapewniać wykrywanie potencjalnie niepożądanych, niebezpiecznych oraz podejrzanych aplikacji.
6. Rozwiązanie musi zapewniać skanowanie w czasie rzeczywistym otwieranych, zapisywanych i wykonywanych plików.
7. Rozwiązanie musi zapewniać skanowanie całego dysku, wybranych katalogów lub pojedynczych plików "na żądanie" lub według harmonogramu.
8. Rozwiązanie musi zapewniać skanowanie plików spakowanych i skompresowanych oraz dysków sieciowych i dysków przenośnych.
9. Rozwiązanie musi posiadać opcję umieszczenia na liście wykluczeń ze skanowania wybranych plików, katalogów lub plików na podstawie rozszerzenia, nazwy, sumy kontrolnej (SHA1) oraz lokalizacji pliku.
10. Rozwiązanie musi zapewniać skanowanie i oczyszczanie poczty przychodzącej POP3 i IMAP „w locie” (w czasie rzeczywistym), zanim zostanie dostarczona do klienta pocztowego, zainstalowanego na stacji roboczej (niezależnie od konkretnego klienta pocztowego).
11. Rozwiązanie musi zapewniać skanowanie ruchu sieciowego wewnątrz szyfrowanych protokołów HTTPS, POP3S, IMAPS.
12. Rozwiązanie musi posiadać wbudowane dwa niezależne moduły heurystyczne – jeden wykorzystujący pasywne

metody heurystyczne i drugi wykorzystujący aktywne metody heurystyczne oraz elementy sztucznej inteligencji. Musi istnieć możliwość wyboru, z jaką heurystyka ma odbywać się skanowanie – z użyciem jednej lub obu metod jednocześnie.

13. Rozwiązanie musi zapewniać blokowanie zewnętrznych nośników danych na stacji w tym przynajmniej: Pamięci masowych, optycznych pamięci masowych, pamięci masowych Firewire, urządzeń do tworzenia obrazów, drukarek USB, urządzeń Bluetooth, czytników kart inteligentnych, modemów, portów LPT/COM oraz urządzeń przenośnych.

14. Rozwiązanie musi posiadać funkcję blokowania nośników wymiennych, bądź grup urządzeń ma umożliwiać użytkownikowi tworzenie reguł dla podłączanych urządzeń minimum w oparciu o typ, numer seryjny, dostawcę lub model urządzenia.

15. 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.

• 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.

16. 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.

17. 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.

18. Rozwiązanie musi posiadać automatyczną, inkrementacyjną aktualizację silnika detekcji.

19. Rozwiązanie musi posiadać tylko jeden proces uruchamiany w pamięci, z którego korzystają wszystkie funkcje systemu (antywirus, antyspyware, metody heurystyczne).

20. Rozwiązanie musi posiadać funkcjonalność skanera UEFI, który chroni użytkownika poprzez wykrywanie i blokowanie zagrożeń, atakujących jeszcze przed uruchomieniem systemu operacyjnego.

21. Rozwiązanie musi posiadać ochronę antyspamową dla programów pocztowych MS Outlook, Outlook Express, Windows Mail oraz Windows Live Mail.

22. Zapora osobista rozwiązania musi pracować w jednym z czterech trybów:

23. Rozwiązanie musi być wyposażona w moduł bezpiecznej przeglądarki.

24. Przeglądarka musi automatycznie szyfrować wszelkie dane wprowadzane przez Użytkownika.

25. Praca w bezpiecznej przeglądarce musi być wyróżniona poprzez odpowiedni kolor ramki przeglądarki oraz informację na ramce przeglądarki.

26. Rozwiązanie musi być wyposażone w zintegrowany moduł kontroli dostępu do stron internetowych.

27. Rozwiązanie musi posiadać możliwość filtrowania adresów URL w oparciu o co najmniej 140 kategorii i podkategorii.

Ochrona serwera

1. Rozwiązanie musi wspierać systemy Microsoft Windows Server 2012 i nowszych oraz Linux w tym co najmniej: RedHat Enterprise Linux (RHEL) 7 i 8, CentOS 7 i 8, Ubuntu Server 16.04 LTS i nowsze, Debian 9, Debian 10, SUSE Linux Enterprise Server (SLES) 12, SUSE Linux Enterprise Server (SLES) 15, Oracle Linux oraz Amazon Linux.
2. Rozwiązanie musi zapewniać ochronę przed wirusami, trojanami, robakami i innymi zagrożeniami.
3. Rozwiązanie musi zapewniać wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor.
4. Rozwiązanie musi zapewniać możliwość skanowania dysków sieciowych typu NAS.
5. Rozwiązanie musi posiadać wbudowane dwa niezależne moduły heurystyczne – jeden wykorzystujący pasywne metody heurystyczne i drugi wykorzystujący aktywne metody heurystyczne oraz elementy sztucznej inteligencji. Rozwiązanie musi istnieć możliwość wyboru, z jaką heurystyka ma odbywać się skanowanie – z użyciem jednej lub obu metod jednocześnie.
6. Rozwiązanie musi wspierać automatyczną, inkrementacyjną aktualizację silnika detekcji.
7. Rozwiązanie musi posiadać możliwość wykluczania ze skanowania procesów.
8. Rozwiązanie musi posiadać możliwość określenia typu podejrzanych plików, jakie będą przesyłane do producenta, w tym co najmniej pliki wykonywalne, archiwa, skrypty, dokumenty

Dodatkowe wymagania dla ochrony serwerów Windows:

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

Dodatkowe wymagania dla ochrony serwerów Linux:

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

Ochrona urządzeń mobilnych opartych o system Android

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

III. Informacje dodatkowe.

1. Zamawiający wymaga załączenia do Formularza ofertowego (załącznik nr 1 do SWZ) wykazu oferowanego sprzętu komputerowego wraz ze szczegółowym opisem technicznym (nazwy, typu, modelu, cech charakterystycznych danego produktu, itp.) w taki sposób, aby Zamawiający mógł jednoznacznie określić szczególne cechy produktu. W przypadku braku wymaganego opisu Zamawiający wezwie do złożenia wyjaśnień oferty.
2. Zamawiający wymaga, aby wykonanie przedmiotu zamówienia nastąpiło na warunkach i zasadach określonych w projektowanych postanowieniach umowy Przedmiot umowy, o którym mowa w §1 powyżej należy dostarczyć do Zamawiającego na adres: Urząd Gminy w Łącku, ul. Gostynińska 2, 09-520 Łąck.
3. O terminie dostawy Wykonawca zobowiązany jest zawiadomić Zamawiającego co najmniej z 2-dniowym wyprzedzeniem. Dostawa przedmiotu umowy odbędzie się w dni robocze, od poniedziałku do czwartku, w godzinach 8:00 -13:00. Datą odbioru będzie przekazanie kompletnego, sprawdzonego sprzętu i podpisanie protokołu odbioru końcowego przez Zamawiającego.

4. W dniu odbioru Wykonawca zapewni dowód dostawy wraz z numerami seryjnymi każdego dostarczonego sprzętu komputerowego.
5. Przedmiot zamówienia Wykonawca dostarczy własnym środkiem transportu, na własny koszt i ryzyko. Za szkody powstałe w czasie transportu pełną odpowiedzialność ponosi Wykonawca.
6. Wykonawca ponosi wszelkie koszty związane z dostarczeniem przedmiotu zamówienia do Zamawiającego oraz odpowiada za przedmiot zamówienia do czasu jego odbioru przez Zamawiającego.
7. Wykonawca zobowiązuje się dostarczyć przedmiot umowy fabrycznie nowy, nieużywany, wolny od wad fizycznych i prawnych z oprogramowaniem oraz wydania dokumentacji dotyczącej dostarczanego przedmiotu umowy takich jak m. in.: certyfikaty atesty, deklaracje zgodności, instrukcje obsługi w języku polskim, dokumenty gwarancyjne i serwisowe, katalog części zamiennych, wymienionych w karcie gwarancyjnej, tak aby możliwa była prawidłowa rejestracja i eksploatacja wszystkich elementów przedmiotu zamówienia. Dostarczany sprzęt komputerowy będzie oryginalnie opakowany. Opakowania nie mogą być naruszone i winny być opisane co do ich zawartości oraz oznakowane symbolem CE, zgodnie z wymogami określonymi m. in. w rozporządzeniu Ministra Rozwoju z dnia 2 czerwca 2016 roku w sprawie wymagań dla sprzętu elektrycznego (Dz. U. z 2016 r. poz. 806).
8. Wszystkie użyte w dokumentach zamówienia wskazania znaków towarowych, patentów lub pochodzenie, które charakteryzują produkty lub usługi dostarczane przez konkretnego Wykonawcę są podane przykładowo i określają jedynie minimalne, oczekiwane parametry jakościowe oraz wymagany standard. Jeśli w opisie przedmiotu zamówienia lub dokumentacji zamówienia zostały użyte ww. wskazania należy traktować je, jako propozycję i towarzyszy im zapis „lub równoważny”. Zamawiający dopuszcza zastosowanie równoważnych materiałów i urządzeń w stosunku do zaprojektowanych z zachowaniem tych samych lub lepszych standardów technicznych, technologicznych lub jakościowych. Ponadto zamienne materiały lub urządzenia przyjęte do wyceny winny spełniać funkcję, jakiej maja służyć; winny być kompatybilne z pozostałymi urządzeniami, aby zespół urządzeń dawał zamierzony efekt; nie mogą wpływać na zmianę rodzaju i zakresu prac.

9. W sytuacji, gdy w dokumentacji zamówienia wskazano normy, oceny techniczne, specyfikacje techniczne i systemy referencji technicznych, o których mowa w art. 101 ust. 1 - 3 ustawy „Pzp", Zamawiający dopuszcza rozwiązania równoważne opisywanym, a w odniesieniu takiemu towarzyszą wyrazu „lub równoważne". Zamawiający dopuszcza zastosowanie rozwiązań równoważnych – pod warunkiem, że zagwarantują one realizacje zamówienia w zgodzie z SWZ i pozwolą na uzyskanie parametrów nie gorszych niż przewidzianych w dokumentacji zamówienia, natomiast Wykonawca zobowiązany jest udowodnić w ofercie, w szczególności za pomocą przedmiotowych środków dowodowych, o których mowa w art. 104-107 ustawy „Pzp", że proponowane rozwiązania w równoważnym stopniu spełniają wymagania określone w opisie przedmiotu zamówienia.
10. Wykonawca ponosi wszelkie koszty związane z zastosowaniem rozwiązań równoważnych.
11. Zamawiający zastrzega sobie prawo sprawdzenia pełnej zgodności parametrów oferowanego sprzętu z wymogami niniejszej SWZ. W tym celu Wykonawcy na wezwanie Zamawiającego dostarczą do siedziby Zamawiającego w terminie 7 dni od daty otrzymania wezwania, próbkę oferowanego sprzętu. W odniesieniu do programowania mogą zostać dostarczone licencje tymczasowe, w pełni zgodne z oferowanymi. Ocena złożonych próbek zostanie dokonana przez Komisję Przetargową na zasadzie spełnia / nie spełnia. Z badania każdej próbki zostanie sporządzony protokół. Pozytywna ocena próbki będzie oznaczała zgodność próbki (oferty) z treścią SWZ. Niezgodność próbki z SWZ chociażby w zakresie jednego parametru podlegającemu badaniu bądź nieprzedłożenie wymaganej próbki w sposób i terminie wymaganym przez Zamawiającego będzie oznaczało negatywny wynik oceny próbki i będzie skutkowało odrzuceniem oferty. Szczegółowy sposób przygotowania i złożenia próbek zostanie dostarczony wykonawcom wraz z wezwaniem do złożenia próbek.