Znak sprawy: ZW.271.3.2022 **Załącznik nr 1 do SWZ**

Opis przedmiotu zapytania

Laptop – 276 szt

Producent:……..

Typ:……..

Model:……..

LP.	NAZWA KOMPONENTU	WYMAGANE MINIMALNE PARAMETRY TECHNICZNE	SPEŁNIA/NIE SPEŁNIA (TAM GDZIE TO DODATKOWO WYMAGANE, INFORMACJE DODATKOWE W POSTACI NAZW WŁASNYCH)
1	Zastosowanie	Komputer mobilny będzie wykorzystywany dla potrzeb aplikacji, edukacyjnych, obliczeniowych, dostępu do Internetu oraz poczty elektronicznej.	
2	Przekątna Ekrenu	15.6” FHD IPS (1920 x 1080), powłoką przeciwodblaskową, jasność 220 nitów. Kąt otwarcia matrycy min.140 stopni	
3	Wydajność komputera	Procesor wielordzeniowy ze zintegrowanym układem graficznym osiągający w teście wydajności PC Mark 10 – wynik min. 2800 pkt – test przeprowadzony na oferowanej konfiguracji należy załączyć do oferty. Wymagane testy wydajnościowe wykonawca musi przeprowadzić na automatycznych ustawieniach konfiguratora dołączonego przez producenta ww oprogramowania i przy natywnej rozdzielczości wyświetlacza oraz włączonych wszystkich urządzaniach. Nie dopuszcza się stosowanie overclokingu, oprogramowania wspomagającego pochodzącego z innego źródła niż fabrycznie zainstalowane oprogramowanie przez producenta, ingerowania w ustawieniach BIOS (tzn. wyłączanie urządzeń stanowiących pełną konfigurację) jak również w samym środowisku systemu (tzn. zmniejszanie rozdzielczości, jasności i kontrastu itp.). Zamawiający zastrzega sobie, iż w celu sprawdzenia poprawności przeprowadzonych wszystkich wymaganych testów Oferent musi dostarczyć Zamawiającemu oprogramowanie testujące, komputer do testu oraz dokładny opis metodyki przeprowadzonego testu wraz z wynikami w celu ich sprawdzenia w terminie nie dłuższym niż 3 dni od otrzymania zawiadomienia od Zamawiającego	Należy podać producenta i model oferowanego procesora:

4	Pamięć RAM	8GB DDR4 z możliwością rozbudowy do min. 32GB RAM. Co najmniej 2 fizyczne gniazda SODIMM DDR4. Wyklucza się pamięć wlutowaną/zintegrowaną z płyta główną.	
5	Pamięć masowa	256GB NVMe SSD M.2 Komputer musi oferować montaż dwóch dysków w konfiguracji M.2 + 2,5”	
6	Karta graficzna	Zintegrowana karta graficzna osiągająca w teście Sysmark25 Creativity co najmniej 580 punktów - wyniki testu przeprowadzonego na oferowanej konfiguracji załączyć do oferty.	
7	Klawiatura	klawiatura w układzie polski programisty, min 100 klawiszy. Wszystkie klawisze funkcyjne typu: mute, regulacja głośności, print screen dostępne w ciągu klawiszy F1-F12.	
8	Multimedia	Karta dźwiękowa zintegrowana z płytą główną, wbudowane dwa głośniki stereo 2x2W. Cyfrowy mikrofon z funkcją redukcji szumów i poprawy mowy wbudowany w obudowę matrycy. Kamera internetowa z diodą informującą o aktywności, trwale zainstalowana w obudowie matrycy. 1 port audio typu combo (słuchawki i mikrofon),	
9	Łączność bezprzewodowa	Wi-Fi 5 AC Bluetooth 5.0	
10	Bateria i zasilanie	Bateria litowo-polimerowa lub litowo-jonowa. Umożliwiająca jej szybkie naładowanie do poziomu 80% w czasie 1 godziny i do poziomu 100% w czasie 2 godzin. Czas pracy na baterii min. 9,5 godziny, potwierdzony przeprowadzonym testem MobileMark25 Battery Life z liczbą przeprowadzonych iteracji min. 4. [do oferty należy załączyć wydruk przeprowadzonego testu dla oferowanej konfiguracji] Zasilacz o mocy min. 45W	
11	Waga i wymiary	Waga max 1.7 kg z baterią Wysokość laptopa nie większa niż 20mm.	
12	Obudowa	Szkielet obudowy i zawiasy notebooka wzmacniane, uszczelnienie chroniące klawiaturę notebooka po zamknięciu przed kurzem i wilgocią	
13	Certyfikaty	Certyfikat ISO9001, ISO 14001, ISO50001 dla producenta sprzętu (należy załączyć do oferty). Potwierdzenie spełnienia kryteriów środowiskowych, w tym zgodności z dyrektywą RoHS Unii Europejskiej o eliminacji substancji niebezpiecznych w postaci oświadczenia producenta jednostki. (należy załączyć do oferty). Potwierdzenie kompatybilności komputera z oferowanym systemem operacyjnym (wydruk ze strony producenta systemu operacyjnego).	

14	Oprogramowanie zabezpieczające	System chroniący przed zagrożeniami, posiadający certyfikaty VB100%, OPSWAT, AVLAB +++, AV Comperative Advance +. Silnik 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, • wykrywanie i usuwanie fałszywego oprogramowania bezpieczeństwa (roguewear) Oprogramowanie umożliwia zdefiniowanie listy zaufanych urządzeń, które nie będą blokowane podczas podłączanie do stacji końcowej. Istnieje możliwość blokady zapisywanie plików na zewnętrznych dyskach USB oraz blokada możliwości uruchamiania oprogramowania z takich dysków. Blokada ta powinna umożliwiać korzystanie z pozostałych danych zapisanych na takich dyskach. Interfejs zarządzania wyświetla monity o zbliżającym się zakończeniu licencji, a także powiadamia o zakończeniu licencji. Oprogramowanie do szyfrowania, chroniące dane rezydujące na punktach końcowych za pomocą silnych algorytmów szyfrowania takich jak AES, RC6, SERPENT i DWAFISH. Pełne szyfrowanie dysków działających m.in. na komputerach z systemem Windows. • Zapobiegające utracie danych z powodu utraty / kradzieży punktu końcowego. Oprogramowanie szyfruje całą zawartość na urządzeniach przenośnych, takich jak Pen Drive'y, dyski USB i udostępnia je tylko autoryzowanym użytkownikom. Zarządzanie przez Chmurę: 1. Musi być zdolny do wyświetlania statusu bezpieczeństwa konsolidacyjnego urządzeń końcowych zainstalowanych w różnych sieciach 2. Musi posiadać zdolność do tworzenia kopii zapasowych i przywracania plików konfiguracyjnych z serwera chmury 3. Musi posiadać zdolność do promowania skutecznej polityki w ramach sieci domowej. 4. Musi mieć możliwość tworzenia wielu poziomów dostępu do hierarchii aby umożliwić dostęp do Chmury zgodnie z przypisaniem do grupy 5. Musi posiadać dostęp do konsoli lokalnie z dowolnego miejsca w nagłych przypadkach Aktualizacja oprogramowania w trybie offline, za pomocą paczek aktualizacyjnych ściągniętych z dedykowanej witryny producenta oprogramowania. 1. Serwer: centralna konsola zarządzająca oraz oprogramowanie chroniące komputery, również w sieci domowej. 2. Oprogramowanie klienckie, zarządzane z poziomu serwera.	Należy podać producenta oraz nazwę oferowanego oprogramowania

System musi umożliwiać, w sposób centralnie zarządzany z konsoli, co najmniej:
- różne ustawienia dostępu dla urządzeń: pełny dostęp, tylko do odczytu i blokowanie
- funkcje przyznania praw dostępu dla nośników pamięci tj. USB, CD
- funkcje regulowania połączeń WiFi i Bluetooth
- funkcje blokowania dostępu dowolnemu urządzeniu
- zdolność do szyfrowania zawartości USB i udostępniania go na punktach końcowych z zainstalowanym oprogramowaniem klienckim systemu
- możliwość zablokowania funkcjonalności portów USB, blokując dostęp urządzeniom innym niż klawiatura i myszka

Monitorowanie zmian w plikach:
- Możliwość monitorowania działań związanych z obsługą plików, takich jak kopiowanie, usuwanie, przenoszenie na dyskach lokalnych, dyskach wymiennych i sieciowych.
- Funkcje monitorowania określonych rodzajów plików.
- Możliwość wykluczenia określonych plików/folderów dla procedury monitorowania.
- Generator raportów do funkcjonalności monitora zmian w plikach.
- możliwość śledzenia zmian we wszystkich plikach
- możliwość śledzenia zmian w oprogramowaniu zainstalowanym na końcówkach
- możliwość definiowana własnych typów plików

Optymalizacja systemu operacyjnego stacji klienckich:
- usuwanie tymczasowych plików, czyszczenie niepotrzebnych wpisów do rejestru oraz defragmentacji dysku
- optymalizacja w chwili startu systemu operacyjnego, przed jego całkowitym uruchomieniem
- możliwość zaplanowania optymalizacje na wskazanych stacjach klienckich
- instruktaż stanowiskowy pracowników Zamawiającego
- dokumentacja techniczna w języku polskim

Moduł oprogramowania pozwalające na wykrywaniu oraz zarządzaniu podatnościami bezpieczeństwa - wymagania dotyczące technologii:
1. Dostęp do rozwiązania realizowany jest za pomocą dedykowanego portalu zarządzającego dostępnego przez przeglądarkę internetową
2. Portal zarządzający musi być dostępny w postaci usługi hostowanej na serwerach producenta.
3. Dostęp do portalu zarządzającego odbywa się za pomocą wspieranych przeglądarek internetowych
4. Rozwiązanie realizuje skany podatności za pomocą dedykowanych nodów skanujących
5. Nod skanujący musi być dostępny w postaci usługi hostowanej na serwerach producenta oraz w postaci aplikacji instalowanej lokalnie
6. Portal zarządzający musi umożliwiać:

a) przegląd wybranych danych na podstawie konfigurowalnych widgetów

		b) zablokowania możliwości zmiany konfiguracji widgetów c) zarządzanie skanami podatności (start, stop), przeglądanie listy podatności oraz tworzenie raportów. d) tworzenie grup skanów z odpowiednią konfiguracją poszczególnych skanów podatności e) eksport wszystkich skanów podatności do pliku CSV Backup i przywracanie danych: a. Deduplikacja danych, b. Backup przyrostowy i różnicowy, c. Wersjonowanie plików – możliwość zdefiniowania dowolnej ilości wersji, d. Backup danych lokalnych – plikowy oraz poczty Outlook, e. Backup otwartych plików (VSS), f. Filtr plików oraz folderów, g. Domyślne wykluczenia zbędnych plików (pliki tymczasowe etc.), h. Wyłączanie komputera po wykonaniu backupu, i. Przywracanie danych do wskazanej lokalizacji, j. Możliwość backup-u z wykorzystaniem dowolnej ilości rdzeni procesora, k. Wyszukiwanie plików w repozytorium użytkownika, l. Automatyczne logowanie, m. Zapamiętywanie danych logowania, n. Automatyczne uruchamianie programu przy starcie systemu, o. Ustawianie priorytetu dla procesu backupu, p. Zmiana klucza szyfrującego, q. Ustawienia przepustowości/zajętości pasma, r. Konfiguracja wydajności procesu backupu, Bezpieczeństwo a. Zastępowanie nazwy pliku GUID-em, b. Szyfrowanie danych algorytmem AES 256 CBC, zawsze po stronie komputera użytkownika, c. Kompresja danych, d. Transmisja po bezpiecznym protokole TLS, e. Deklaracja klucza szyfrującego dane użytkownika, f. Szczegółowy dziennik zdarzeń dostępny z poziomu aplikacji, g. Obliczanie sumy kontrolnej, Kopie zapasowe są przechowywane w profesjonalnych, certyfikowanych data center, na terenie Polski. WSPIERANE SYSTEMY OPERACYJNE Microsoft Windows 10 i nowsze, Mac OS,Licencje przypisywane do jednego urządzenia z limitem pojemności przestrzeni w chmurze – minimum 50 GB. Wsparcie techniczne, świadczone w języku polskim, zawarte jest w cenie licencji	
16	Diagnostyka	System diagnostyczny z graficznym interfejsem użytkownika dostępny z poziomu BIOS lub z poziomu menu boot, umożliwiający przetestowanie komponentów komputera. Pełna funkcjonalność systemu diagnostycznego musi być realizowana	

		bez użycia : dostępu do sieci i internetu, dysku twardego również w przypadku jego braku, urządzeń zewnętrznych i wewnętrznych typu : pamięć flash, USBpen itp.	
17	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.	
18	System operacyjny – w formularzu oferty należy podać pełną nazwę oferowanego oprogramowania	Oferowany komputer musi zostać dostarczony z licencją oprogramowania systemu operacyjnego klasy Microsoft Windows 10 HOME lub równoważny. Za równoważny system operacyjny Zamawiający uzna system spełniający następujące minimalne parametry: Możliwość dokonywania aktualizacji i poprawek systemu przez Internet; możliwość dokonywania uaktualnień sterowników urządzeń przez Internet – witrynę producenta systemu; Darmowe aktualizacje w ramach wersji systemu operacyjnego przez Internet (niezbędne aktualizacje, poprawki, biuletyny bezpieczeństwa muszą być dostarczane bez dodatkowych opłat) – wymagane podanie nazwy strony serwera WWW; Internetowa aktualizacja zapewniona w języku polskim; Wbudowana zapora internetowa (firewall) dla ochrony połączeń internetowych; zintegrowana z systemem konsola do zarządzania ustawieniami zapory i regułami IPSec v4 i v6; Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, przeglądarka internetowa, pomoc, komunikaty systemowe; Wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (np.: drukarek, urządzeń sieciowych, standardów USB, Plug&Play, Wi-Fi); Zabezpieczony hasłem hierarchiczny dostęp do systemu, konta i profile użytkowników zarządzane zdalnie; praca systemu w trybie ochrony kont użytkowników; Zintegrowany z systemem moduł wyszukiwania informacji (plików różnego typu) dostępny z kilku poziomów: poziom menu, poziom otwartego okna systemu operacyjnego; system wyszukiwania oparty na konfigurowalnym przez użytkownika module indeksacji zasobów lokalnych; Zintegrowane z systemem operacyjnym narzędzia zwalczające złośliwe oprogramowanie; aktualizacje dostępne u producentanieodpłatnie bez ograniczeń czasowych; Wbudowany system pomocy w języku polskim; System operacyjny powinien być wyposażony w możliwość przystosowania stanowiska dla osób niepełnosprawnych	Należy podać producenta oraz nazwę oferowanego systemu operacyjnego:

		(np. słabo widzących); Możliwość zarządzania stacją roboczą poprzez polityki – przez politykę rozumiemy zestaw reguł definiujących lub ograniczających funkcjonalność systemu lub aplikacji; System posiadać powinien narzędzia służące do administracji, do wykonywania kopii zapasowych polityk i ich odtwarzania oraz generowania raportów z ustawień polityk; Zarządzanie kontami użytkowników sieci oraz urządzeniami sieciowymi tj. drukarki, modemy, woluminy dyskowe, usługi katalogowe; Możliwość przywracania plików systemowych. Zamawiający nie dopuszcza licencji edukacyjnych STF.	
19	Porty i złącza	Wbudowane porty i złącza: 1x HDMI 1.4 1x RJ-45, 3x USB w tym min. 2x USB 3.2, port zasilania, złącze linki zabezpieczającej typu kensington.	
20	Warunki gwarancyjne, wsparcie techniczne	Dedykowany portal techniczny producenta, umożliwiający Zamawiającemu zgłaszanie awarii oraz samodzielne zamawianie zamiennych komponentów. 2-letnia gwarancja, czas reakcji serwisu do końca następnego dnia roboczego. Gwarancja musi oferować przez cały okres : - mieć opiekę kierownika technicznego ds. Eskalacji - dostępność wsparcia technicznego przez 24 godziny 7 dni w tygodniu przez cały rok (w języku polskim w dni robocze) Firma serwisująca musi posiadać ISO 9001:2000 na świadczenie usług serwisowych oraz posiadać autoryzacje producenta komputera.	

Zestaw Komputerowy PC – 49 szt

Producent:……..

Typ:……..

Model:……..

Lp.	Nazwa komponentu	Wymagane minimalne parametry techniczne	Parametry oferowane (należy podać dokładnie rzeczywiste oferowane parametry, oraz tam gdzie to dodatkowo wymagane, informacje dodatkowe w postaci nazw własnych)
1.	Komputer	Komputer będzie wykorzystywany dla potrzeb aplikacji biurowych, dostępu do Internetu oraz poczty elektronicznej, jako lokalna baza danych, stacja programistyczna. W ofercie należy podać nazwę producenta, typ, model, oferowanego sprzętu.	
2.	Obudowa	Typu tower lub SFF z obsługą kart PCI Express wyłącznie o wysokim (pełnym) profilu. Fabrycznie umożliwiająca montaż min. - 1 szt. zewnętrzna 5,25” na napęd optyczny (dopuszcza się stosowanie napedów slim) - wewnątrz, min. 5 szt. (2,5” / 3,5” - dyski twarde SSD/HDD) - Obudowa trwale oznaczona nazwą producenta, nazwą komputera, numerem seryjnym - Suma wymiarów obudowy nie może być większa niż 975 mm. - konstrukcja obudowy wymuszająca cyrkulację powietrza od przodu do tyłu (wyklucza się otwory na panelach bocznych) - bezpośrednio z przodu obudowy fabrycznie zintegrowane wyjścia/złącza:	Należy podać producenta i model:

		2 x USB 3.0, wyjście słuchawkowe, wejście mikrofonowe, czytnik kart multimedialnych SD oraz microSD (bez konieczności stosowania adapterów kart) - obudowa fabrycznie wyposażona w filtr przeciwkurzowy	
3.	Zasilacz	- Zasilacz o mocy minimalnej 400W oraz wysokiej sprawności minimum 90% przy 50% obciążeniu (na podstawie danych z certyfikatu 80PLUS) - Zasilacz posiadający certyfikat 80PLUS GOLD. - aktywne PFC - żywotność min. 100000 godzin - wentylator o średnicy min. 120 mm - wyposażony w zabezpieczenia: nadmiarowo-prądowe, nadmiarowo-napięciowe, niedomiarowo-napięciowe, zwarciowe, temperaturowe, przeciążeniowe	Należy podać producenta i model:
4.	Chipset	Dostosowany do zaoferowanego procesora	Należy podać producenta i model:
5.	Płyta główna	Zaprojektowana i wyprodukowana przez producenta. Wyposażona w złącza min.: - 1 x PCI Express 3.0 x16, - 1 x PCI Express 3.0 x1, - 1 x M.2 - 4 x SATA 6Gb/s Złącza na panelu tylnym - 2 porty PS/2 - 1 port D-Sub - 1 port DVI-D - 1 port HDMI - 2 porty USB 3.2 Gen 1 - 4 porty USB 2.0 - 1 port RJ-45 - 3 gniazda audio	
6.		Procesor wielordzeniowy ze zintegrowaną grafiką, zaprojektowany do pracy w komputerach stacjonarnych klasy x86, o wydajności min. 2800	Należy podać producenta i model:

	Procesor	pkt. liczonej na podstawie PerformanceTest w teście CPU Mark według wyników Avarage CPU Mark opublikowanych na http://www.cpubenchmark.net/. (Wynik aktualny w okresie od ukazania się ogłoszenia niniejszego postępowania do dnia otwarcia ofert). Wykonawca w składanej ofercie winien podać dokładny model oferowanego podzespołu.	
7.	Pamięć operacyjna	Min. 8GB DDR4 z możliwością rozszerzenia do 64 GB Ilość wolnych banków pamięci: min. 1 szt.	
8.	Dysk twardy	Min 512 GB SSD M.2 PCIe NVMe zawierający recovery umożliwiające odtworzenie systemu operacyjnego fabrycznie zainstalowanego na komputerze po awarii. MTBF min. 2 mln godzin TBW min. 330 TB	Należy podać producenta i model:
9.	Napęd optyczny	Wbudowana w obudowę komputera Nagrywarka DVD +/-RW	
10.	Karta graficzna	Zintegrowana karta graficzna wykorzystująca pamięć RAM systemu dynamicznie przydzielaną na potrzeby grafiki w trybie UMA (Unified Memory Access) – z możliwością dynamicznego przydzielenia pamięci.	
11.	Audio	Karta dźwiękowa zintegrowana z płytą główną, zgodna z High Definition.	
12.	Karta sieciowa	LAN 100/1000 Mbit/s z funkcją PXE oraz Wake on LAN	
13.	Klawiatura/mysz	Klawiatura - przewodowa (długość przewodu min. 1,8m) - układ QWERTY - odporna na przypadkowe zalanie płynami (min. 50 ml) - cienki profil - trwałe klawisze (min. 10 milionów naciśnięć) - Wytrzymałe, odchylane nóżki (nachylenie min. 8 stopni)	Należy podać producenta i model:

		- ergonomiczna zakrzywiona spacja Mysz - optyczna - przewodowa (długość przewodu min. 1,8m) - rozdzielszość min. 1000 dpi	
14.	System operacyjny – w formularzu oferty należy podać pełną nazwę oferowanego oprogramowania	Fabrycznie zainstalowany przed producenta komputera 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 wielu językach do wyboru – w tym 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 kilku poziomów: poziom menu, poziom otwartego okna systemu	Należy podać producenta oraz nazwę oferowanego systemu operacyjnego:

		operacyjnego; system wyszukiwania oparty na konfigurowalnym przez użytkownika module indeksacji zasobów lokalnych, 7. Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, pomoc, komunikaty systemowe, menedżer plików. 8. Graficzne środowisko instalacji i konfiguracji dostępne w języku polskim 9. Wbudowany system pomocy w języku polskim. 10. Możliwość przystosowania stanowiska dla osób niepełnosprawnych (np. słabo widzących). 11. Możliwość dokonywania aktualizacji i poprawek systemu poprzez mechanizm zarządzany przez administratora systemu Zamawiającego. 12. Możliwość dostarczania poprawek do systemu operacyjnego w modelu peer-to-peer. 13. Możliwość sterowania czasem dostarczania nowych wersji systemu operacyjnego, możliwość centralnego opóźniania dostarczania nowej wersji o minimum 4 miesiące. 14. Zabezpieczony hasłem hierarchiczny dostęp do systemu, konta i profile użytkowników zarządzane zdalnie; praca systemu w trybie ochrony kont użytkowników. 15. Możliwość dołączenia systemu do usługi katalogowej on-premise lub w chmurze. 16. Umożliwienie zablokowania urządzenia w ramach danego konta tylko do uruchamiania wybranej aplikacji - tryb "kiosk". 17. 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. 18. Zdalna pomoc i współdzielenie aplikacji – możliwość zdalnego przejęcia sesji zalogowanego użytkownika celem rozwiązania problemu z komputerem. 19. Transakcyjny system plików pozwalający na stosowanie przydziałów (ang. quota) na dysku dla użytkowników oraz zapewniający większą niezawodność i pozwalający tworzyć kopie zapasowe. 20. Oprogramowanie dla tworzenia kopii zapasowych (Backup); automatyczne wykonywanie kopii plików z możliwością automatycznego przywrócenia wersji wcześniejszej. 21. Możliwość przywracania obrazu plików systemowych do uprzednio zapisanej postaci. 22. Możliwość przywracania systemu operacyjnego do stanu początkowego z pozostawieniem plików użytkownika. 23. Możliwość blokowania lub dopuszczania dowolnych urządzeń peryferyjnych za pomocą polityk grupowych (np. przy użyciu numerów identyfikacyjnych sprzętu)." 24. Wbudowany mechanizm wirtualizacji typu hypervisor." 25. Wbudowana możliwość zdalnego dostępu do systemu i pracy zdalnej z wykorzystaniem pełnego interfejsu graficznego.	

	26. Dostępność bezpłatnych biuletynów bezpieczeństwa związanych z działaniem systemu operacyjnego. 27. Wbudowana zapora internetowa (firewall) dla ochrony połączeń internetowych, zintegrowana z systemem konsola do zarządzania ustawieniami zapory i regułami IP v4 i v6. 28. 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.). 29. Możliwość zdefiniowania zarządzanych aplikacji w taki sposób aby automatycznie szyfrowały pliki na poziomie systemu plików. Blokowanie bezpośredniego kopiowania treści między aplikacjami zarządzanymi a niezarządzanymi. 30. Wbudowany system uwierzytelnienia dwuskładnikowego oparty o certyfikat lub klucz prywatny oraz PIN lub uwierzytelnienie biometryczne. 31. Wbudowane mechanizmy ochrony antywirusowej i przeciw złośliwemu oprogramowaniu z zapewnionymi bezpłatnymi aktualizacjami. 32. Wbudowany system szyfrowania dysku twardego ze wsparciem modułu TPM 33. Możliwość tworzenia i przechowywania kopii zapasowych kluczy odzyskiwania do szyfrowania dysku w usługach katalogowych. 34. Możliwość tworzenia wirtualnych kart	

		inteligentnych. 35. Wsparcie dla firmware UEFI i funkcji bezpiecznego rozruchu (Secure Boot) 36. Wbudowany w system, wykorzystywany automatycznie przez wbudowane przeglądarki filtr reputacyjny URL. 37. Wsparcie dla IPSEC oparte na politykach – wdrażanie IPSEC oparte na zestawach reguł definiujących ustawienia zarządzanych w sposób centralny. 38. Mechanizmy logowania w oparciu o: a. Login i hasło, b. Karty inteligentne i certyfikaty (smartcard), c. Wirtualne karty inteligentne i certyfikaty (logowanie w oparciu o certyfikat chroniony poprzez moduł TPM), d. Certyfikat/Klucz i PIN e. Certyfikat/Klucz i uwierzytelnienie biometryczne 39. Wsparcie dla uwierzytelniania na bazie Kerberos v. 5 40. Wbudowany agent do zbierania danych na temat zagrożeń na stacji roboczej. 41. Wsparcie .NET Framework 2.x, 3.x i 4.x – możliwość uruchomienia aplikacji działających we wskazanych środowiskach 42. Wsparcie dla VBScript – możliwość uruchamiania interpretera poleceń 43. Wsparcie dla PowerShell 5.x – możliwość uruchamiania interpretera poleceń **Zamawiający nie dopuszcza licencji**	

		edukacyjnych STF.	
15.	Oprogramowanie zabezpieczające - – w formularzu oferty należy podać pełną nazwę oferowanego oprogramowania	System ochrony poczty elektronicznej: System musi zapewniać ochronę przed zagrożeniami związanymi z przesyłaniem poczty elektronicznej (wirusy, spam, phishing, niedozwolone treści, etc.). System musi być dostarczony w zamkniętego rozwiązania sprzętowego lub obrazu maszyny wirtualnej. Zarządzanie lokalne i zdalne systemem musi być możliwe przy użyciu bezpiecznego połączenia HTTPS przez przeglądarkę internetową oraz poprzez protokół SSH. System musi umożliwiać pracę w architekturze Master-Agent oraz przypisanie profilów dla poszczególnych agentów. System musi pracować jako brama SMTP i być niezależnym od rodzaju stosowanego, chronionego serwera poczty. System musi umożliwiać filtrowanie poczty przychodzącej dla wskazanych domen oraz przesyłanie ruchu pocztowego na wskazanych serwer pocztowy. System musi umożliwiać filtrowanie poczty wychodzącej do wskazanych przez Administratora serwerów pocztowych/domen. System musi zapewnić możliwość zdefiniowania osobnych tras przesyłania poczty dla ruchu przychodzącego i wychodzącego w oparciu o statyczne wpisy adresów serwerów, smart hosta lub rekordy MX serwerów DNS. Administrator musi mieć możliwość zapisu konfiguracji na zewnętrzny nośnik i odtworzenia konfiguracji. System musi umożliwiać automatyczne wykonywanie kopii zapasowej konfiguracji zgodnie z harmonogramem. System w momencie dostarczenia lub po odtworzeniu musi zawierać zestaw predefiniowanych reguł i polityk dla wszystkich modułów filtrujących: AV, antyspam, kontrola treści. System musi umożliwiać automatyczne pobieranie oraz instalowanie aktualizacji modułów ochronnych oraz całego systemu. Wszystkie aktualizacje muszą być pobierane z jednego miejsca a system komunikować się ze źródłem aktualizacji z częstotliwością narzuconą	Należy podać nazwę producenta, nazwę oraz wersję oferowanego oprogramowania dodatkowego:

		przez administratora systemu. System musi zapewnić śledzenie historii wykonywania aktualizacji. Producent musi zapewnić możliwość zakupu aktualizacji systemu jednorazowo na okres roku, dwóch lub trzech lat. System musi umożliwiać tworzenie wielu administratorów oraz przypisanie im odpowiednich uprawnień dostępowych do modułów ochronnych. System musi zapewniać rozbudowany system raportowania zapewniający dostęp do minimum 65 różnych rodzajów graficznych raportów oraz możliwość tworzenia własnych. System w momencie dostarczenia lub po odtworzeniu musi zawierać zestaw predefiniowanych raportów. Administrator musi mieć możliwość okresowej publikacji wybranych raportów jako strony WWW lub przy pomocy wysyłanych automatycznie wiadomości email. System musi umożliwiać eksport logów do formatu CSV oraz XML. System musi umożliwiać logowanie na lokalnym dysku twardym lub zewnętrznym serwerze Syslog zdarzeń podejmowanych przez filtry oraz zdarzeń dotyczących komunikacji SMTP. System musi posiadać lokalną kwarantannę dla zainfekowanych wiadomości. System musi zapewniać możliwość zarządzania użytkownikom końcowymi wiadomościami trafiającymi do ich personalnej kwarantanny. System musi umożliwiać określanie poziomu dostępu i akcji możliwych do wykonania w obrębie kwarantanny dla różnych użytkowników/grup użytkowników. Kwarantanna użytkownika oraz skrócone informacje o stanie kwarantanny dla użytkownika muszą być dostępne w języku polskim. System musi zapewniać możliwość opcjonalnego uwierzytelniania użytkownika w celu zmian parametrów własnego folderu kwarantanny. System musi zapewniać możliwość definiowania list zaufanych i blokowanych nadawców przez użytkowników końcowych. System musi umożliwiać definiowanie wyglądu kwarantanny końcowego użytkownika zarówno, co do jej szaty graficznej (np. możliwość umieszczenia znaku firmowego) jak i treści komunikatów. System musi umożliwiać definiowanie i	

		przeglądanie wielu katalogów kwarantanny dla różnych reguł antywirusowych i antyspamowych. Dla wszystkich stworzonych folderów kwarantanny system musi zapewniać możliwość ustawienia maksymalnego czasu przechowywania wiadomości a po jego upływie automatycznie je usunie. System musi umożliwiać wyszukiwanie wiadomości w kwarantannie na podstawie nadawcy, odbiorcy, tematu wiadomości lub czasu od kiedy wiadomość znajduje się w kwarantannie. System musi umożliwiać następujące operacje na wiadomościach przechowywanych w obszarze kwarantanny: usunięcie wiadomości, przesłanie do innego odbiorcy, przeniesienie do innego folderu, zwolnienie wiadomości, zwolnienie zaszyfrowanej wiadomości. Urządzenie musi zapewnić możliwość zgłoszenia przypadków złej klasyfikacji wiadomości do producenta systemu na poziomie kwarantanny administratora oraz personalnej kwarantanny użytkownika końcowego. Listy użytkowników definiowane lokalnie, możliwość importu użytkowników z serwerów: Active Directory, LDAP, MS Exchange, Lotus Domino oraz plików (tekstowe, csv). Możliwość ustawienia harmonogramu importowania użytkowników przez administratora. Możliwość tworzenia grup użytkowników oraz przypisywania im odpowiedniej konfiguracji. Możliwość wysyłania użytkownikom wiadomości powitalnej informującej o dodaniu użytkownika do systemu oraz zawierającej bezpośredni link do konta użytkownika w systemie oraz tymczasowe hasło dostępu. System musi umożliwiać konfigurację harmonogramu wysyłania powiadomień mailowych do użytkowników o np. nowych elementach w kwarantannie. System musi posiadać graficzny interfejs dla administratora do śledzenia przesyłek na MTA i modułach filtrujących na podstawie parametrów: odbiorca, nadawca, nazwa załącznika, temat wiadomości, sender hostname lub IP, QID, RuleID, Message ID, nazwa wirusa, SID. System musi zapewniać możliwość tworzenia własnych reguł filtrowania treści w oparciu o: adresy IP nadawców odbiorców, adresy email, typ i rozmiar załącznika, ilość załączników, treść maila,	

		pola nagłówka wiadomości, treść załączników. System musi umożliwiać tworzenia nowych reguł lub klonowania obecnych. System musi umożliwiać tworzenie słowników słów kluczowych. System musi umożliwiać weryfikację odbiorcy na podstawie LDAP, SMTP lub repozytorium użytkowników. System musi zapewniać wsparcie dla standardu Sender Policy Framework (SPF). System musi zapewniać wsparcie dla autentykacji DomainKeys Identified Mail (DKIM). Ochrona antywirusowa musi być realizowana poprzez silniki zasilane w sygnatury oraz filtr analizy heurystycznej wykrywający ataki typu zero hour. System musi umożliwiać przegląd ostatnich infekcji oraz listę najczęstszych wykrytych zagrożeń. Aktualizacje sygnatur modułu antywirusowego muszą być dostępne nie rzadziej niż raz na dobę. System musi zapewniać możliwość tworzenia kilku polityk ochrony antywirusowej przydzielanych w oparciu o: adresy IP serwera nadawcy, adres email nadawcy/odbiorcy wiadomości Możliwość definiowania różnych sposobów postępowania z zainfekowanymi wiadomościami w zależności od rodzaju wykrytego wirusa Możliwość określenia postępowania z zabezpieczonymi wiadomościami (załączniki chronione hasłem, podpisane wiadomości, etc.) Moduł detekcji spamu musi bazować na metodzie zaawansowanej analizy heurystycznej, która wyklucza konieczność ręcznego tworzenia reguł w razie pojawienia się nowych technik omijania filtrów antyspamowych. System musi umożliwiać korzystanie ze źródeł producenta, niepublicznych serwerów badania reputacji nadawców maila. System musi zapewniać automatyczną ocenę reputacji źródła przesyłanego maila (na podstawie ilości połączeń, procentowej ilości maili z wirusami, procentowej ilości wiadomości sklasyfikowanych jako spam). Możliwość definiowania reguły antyspamowych na poziomie całego urządzenia, grup użytkowników oraz pojedynczych użytkowników. Możliwość tworzenia bezpiecznych i blokowanych list na podstawie odbiorcy, nadawcy, domeny lub	

		adresu IP. System musi zapewniać inteligentne rozpoznawanie typów analizowanych załączników. Zmiana rozszerzeń powinna być ignorowana przez urządzenie i nie powinno być metodą omijania tego typu filtra. System musi zapewniać ochronę przeciwko atakom typu Odmowa dostępu do usług (Denial Of Service) oraz logować i zapobiegać enumeracji kont użytkowników chronionej domeny pocztowej (Directory Harvesting Attack). System musi posiadać mechanizm ochrony (np. cyfrowe oznaczenie maila wychodzacego z organizacji) przed zjawiskiem wykorzystania wiadomosci niedostarczonych (fake NDR) non delivery raports. System musi zapewniać możliwość szyfrowania przesyłek za pomocą protokołu Transport Layer Security. System do ochrony przed wyciekiem poufnych informacji (DLP): System musi posiadać moduł DLP dla ruchu SMTP. System musi umożliwiać przeglądanie incydentów DLP oraz ich wyszukiwanie na podstawie odbiorcy, nadawcy, tematu wiadomości lub typu. System musi umożliwiać tworzenie słowników wzorców informacji poufnych np. numerów kart bankowych, numerów identyfikacyjnych. Możliwość tworzenia reguł na podstawie słowników oraz identyfikatorów informacji poufnych dla poszczególnych państw. Administrator musi mieć możliwość odrzucenia, przekierowania lub zaszyfrowania wiadomości spełniającej warunki reguły DLP. System musi umożliwiać stworzenie repozytorium poufnych dokumentów. Administrator ma możliwość dodania źródeł poufnych dokumentów za pomocą WebDav. System musi umożliwiać ręczne dodanie dokumentów do repozytorium. System umożliwia stworzenie kategorii poufnych dokumentów z możliwością określenia czasu ich wygaśnięcia. Moduł szyfrowania poczty elektronicznej:	

		System musi umożliwiać szyfrowanie wiadomości email bez konieczności instalacji dodatkowego oprogramowania/agenta na serwerze oraz komputerach użytkowników. System działa jak brama szyfrująca oraz miejsce gdzie zaszyfrowana wiadomość jest odczytywana System szyfrowania musi umożliwiać ustawianie czasu do kiedy wiadomość wysłana jest możliwa do odczytania przez odbiorcę Administrator może ustalić czy wiadomość zaszyfrowana może być dalej przekazywana przez oryginalnego odbiorcę do innych odbiorców (forward) czy tylko możliwa jest odpowiedź do nadawcy (Reply, Reply All) Użytkownik może odczytać zaszyfrowaną wiadomość za pomocą bezpiecznego czytnika dostępnego przez przeglądarkę internetową. Użytkownik otrzymuje możliwość odczytania zaszyfrowanej wiadomości w przeglądarce po uwierzytelnieniu się nazwą użytkownika i hasłem. Wzorzec wiadomości zaszyfrowanej dla odbiorców musi być konfigurowalny, co do treści i wyglądu	
16.	Certyfikaty i standardy	- Certyfikat ISO 9001 dla producenta sprzętu (należy załączyć do oferty) - Certyfikat ISO 14001 dla producenta sprzętu (należy załączyć do oferty) - Deklaracja zgodności CE (załączyć do oferty) - Głośność jednostki mierzona z pozycji operatora w trybie IDLE nie większa niż 23 dB – dołączyć dokument potwierdzający głośność jednostki - Potwierdzenie spełnienia kryteriów środowiskowych, w tym zgodności z dyrektywą RoHS Unii Europejskiej o eliminacji substancji niebezpiecznych w postaci oświadczenia producenta jednostki - Certyfikat 80PLUS dla zaoferowanego zasilacza (załączyć do oferty)	-
17.	Bezpieczeństwo	- Złącze typu Kensington Lock	-
18.	Gwarancja	2 lata - Firma serwisująca musi posiadać ISO 9001 oraz ISO 14001 na świadczenie usług serwisowych oraz posiadać autoryzacje producenta urządzeia – dokumenty potwierdzające należy załączyć do oferty.	
19.	Monitor	- Przekątna ekranu min. 21,5”	Należy podać producenta i

		- rozdzielczość min. 1920 x 1080 przy odświeżaniu min. 75Hz - jasność min. 250 cd/m2 - kontrast typowy min. 2500:1 - Czas reakcji maks. 5ms - kąty widzenia pion/poziom min. 178º/178º - wbudowana fabrycznie technologia ograniczająca efekt migotania - wbudowana fabrycznie technologia ograniczająca emisję niebieskiego światła - gniazda wejściowe co najmniej VGA oraz HDMI, wyjście słuchawkowe, wejście audio - wbudowane głośniki min. 2 x 2W (dopuszcza się zaoferowanie dedykowanej przez producenta listwy głośnikowej) - gniazdo zabezpieczające przed kradzieżą typu kensington - mocowanie VESA - podstawa umożliwiająca regulację pochylenia monitora co najmniej w zakresie 25 stopni - zużycie energii w trybie włączenia nie większe niż 14W (na podstawie testu EnergyStar) - waga monitora wraz z podstawą nie przekraczająca 2,6 kg - deklaracja zgodności CE (należy załączyć do oferty) - certyfikat ISO 9001 dla producenta (należy załączyć do oferty) - certyfikat ISO 9001 dla producenta (należy załączyć do oferty)	model:
20.	Wymagania dodatkowe	Zamawiający zastrzega sobie prawo sprawdzenia pełnej zgodności parametrów oferowanego sprzętu z wymogami niniejszej SIWZ. W tym celu Wykonawcy na wezwanie Zamawiającego dostarczą do siedziby Zamawiającego w terminie 3 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 SIWZ. Niezgodność próbki z SIWZ 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 na podstawie art. 89 ust. 1 pkt 2 ustawy z dnia 29 stycznia 2004 r. Prawo zamówień publicznych (Dz. U. z 2015 r. poz. 2164 ze zm.), tj. z uwagi na fakt, że treść oferty nie odpowiada treści specyfikacji istotnych warunków zamówienia. Szczegółowy sposób przygotowania i złożenia próbek zostanie dostarczony wykonawcom wraz z wezwaniem do złożenia próbek	

TABLET – 16 szt

Producent:……..

Typ:……..

Model:……..

Lp.	Nazwa komponentu	Wymagane minimalne parametry techniczne	Parametry oferowane (należy podać dokładnie rzeczywiste oferowane parametry, oraz tam gdzie to dodatkowo wymagane, informacje dodatkowe w postaci nazw własnych)
21.	ekran	Przekątna ekranu Min. 10” Rozdzielczość Min. 1900 x 1100 Matryca IPS lub VA Panel dotykowy pojemnościowy	
22.	Zasilanie oraz Bateria	W zestawie dołączony fabryczny zasilacz (ładowarka) Pojemność wbudowanej baterii min. 5900 mAh	
23.	Procesor	Co najmniej 8 rdzeniowy	
24.	Pamięć operacyjna RAM	Min. 4 GB	
25.	Pamięć wewnętrzna	Min 64 GB	
26.	Karta graficzna	Zintegrowana karta graficzna	
27.	Audio	Wbudowany głośnik Wbudowany mikrofon Wbudowane Radio	
28.	Łączność	Wbudowany GPS	

		Wbudowany modem 4G LTE Wbudowane WiFi 802.11 AC Wbudowany Bluetooth (wersja min. 5.0)	
29.	Porty/złącza	Wbudowane porty/złącza: - USB typ C - gniazdo SIM - wyjście audio (min jack 3,5mm) - czytnik kart micro SD	
30.	System operacyjny	Fabrycznie zainstalowany system operacyjny MS Windows (wersja min. 10) lub Android (wersja min. 11)	Należy podać producenta oraz nazwę oferowanego systemu operacyjnego:
31.	Certyfikaty i standardy	- Deklaracja zgodności CE (załączyć do oferty, dopuszcza się w j. angielskim)	
32.	Waga/rozmiary urządzenia	Grubość tabletu wraz z wbudowaną baterią nie może być większa niż 10mm Tablet wraz z wbudowaną baterią nie może ważyć więcej niż 535g	
33.	Gwarancja	2 lata	
34.	Oprogramowanie do zabezpieczenia tableta	• Oprogramowanie powinno pozwalać na pełne skanowanie oraz szybkie skanowanie • Stałe skanowanie w tle • Skanowanie w celu wykrycia zagrożeń typu malware • Oprogramowanie powinno skanować karty pamięci • Oprogramowanie powinno pozwolić na wyznaczenie wyjątków od skanowania na poziomie tak plików jak i folderów.	Należy podać producenta, nazwę oraz wersję oferowanego oprogramowania do zabezpieczenia tableta:

		• Oprogramowanie powinno analizować zainstalowane aplikacja na urządzenia pod kątem luk w bezpieczeństwie oraz raportować o wystąpieniu o takiej aplikacji. • Oprogramowanie powinno posiadać harmonogram skanowania • Harmonogram skanowania powinien mieć możliwość wywołania skanowania w chwili wykrycia że urządzenie jest ładowane • Oprogramowanie powinno analizować ustawienia urządzenia w celu minimalizowania zagrożeń oraz przekierowywać do ustawień które powinny być zamienione. • Oprogramowanie powinno analizować ustawienia następujących funkcji o Konta i synchronizacja o Bluetooth o Szyfrowanie pamięci urządzenia o Hotspot i Tethering o Blokada ekranu o Nieznane źródła aplikacji o Debugowanie USB o Wi-Fi • Oprogramowanie powinno analizować i monitorować uprawnienia aplikacji do urządzenia takie jak o Dostęp do kontaktów o Dostęp do danych identyfikacyjnych o Śledzenie lokalizacji o Dostęp do wiadomości	

		o Dostęp do sieci • Oprogramowanie powinno chronić przeglądanie Internetu • Oprogramowanie powinno chronić przez atakami typu Phishing. • Oprogramowanie powinno posiadać funkcję optymalizacji urządzenia • Oprogramowanie powinno analizować uruchomione aplikacje i potrafić je zamykać aplikacje nieużywane • Oprogramowanie powinno wspomagać zarządzaniem energią poprzez zamykanie nie używanych aplikacji, kontrolę jasności ekranu, kontrole WiFi, bluetooth. • Oprogramowanie powinno pozwalać na tworzenie dokładnych raportów takich jak wykorzystanie CPU, żywotność baterii oraz wykorzystanie pamięci. • Oprogramowanie powinno mieć funkcjonalność białej listy aplikacji które nie powinny być zatrzymywane. • Oprogramowanie powinno posiadać funkcję monitorowanie sieci, wykorzystania sieci, informować o zbliżającym się limicie danych oraz blokowanie w przypadku osiągnięcia limitu transmisji danych. • Oprogramowanie powinno móc wykonać kopię zapasową w chmurze. • Oprogramowanie powinno móc odzyskać kopię zapasową z chmury. • Urządzenie powinno posiadać funkcję bezpiecznego usunięcia danych z urządzenia i wszystkich jego nośników. • Oprogramowanie powinno posiadać filtr nr. Dzwoniących, w celu odrzucania połączeń niechcianych	

		• Oprogramowanie powinno wspierać blokowanie nieznanych przychodzących połączeń międzynarodowych. • Oprogramowanie powinno zabezpieczać dzienniki połączeń oraz dzienniki wysłanych SMS • Oprogramowanie powinno mieć funkcjonalność ochrony rodzicielskiej która to posiada funkcję o Blokowania stron po kategoriach (oprogramowanie, media społecznościowe, tylko dla dorosłych itp.) o Blokowanie stron z wyszczególnionego adresu URL o Funkcja a powinna wspierać różne przeglądarki internetowe dla Android(Chrome, Firefox, Maxthon, Opera i Dolphin. o Musi posiadać funkcje wyjątków adresów URL • Jeżeli urządzenie wspiera odczytywanie linii papilarnych powinno wspierać takie uwierzytelnianie w celu dostępu do funkcjonalności. • Oprogramowanie powinno posiadać centrum informacji w którym producent informował by o nowych aktualizacjach i ważnych alarmach bezpieczeństwa. • Oprogramowanie powinno wykonywać raporty: o Znalezione wirusy o Zablokowanie połączenia 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 • Oprogramowanie powinno pozwalać na zdalne pobieranie lokalizacji urządzenia • W przypadku zmiany karty SIM oprogramowanie powinno samoistnie wysłać SMS o tym fakcie pod wskazany nr telefonu • Oprogramowanie powinno zablokować urządzenie w przypadku zmiany karty SIM • Oprogramowanie powinno pozwolić na zdalne usuniecie danych z telefonu np.: w przypadku kradzieży. • Oprogramowanie powinno potrafić zadzwonić dyskretnie pod wskazany nr telefonu w celu słuchania dźwięków otoczenia. • Oprogramowanie powinno potrafić rozpoznać i dyskretnie odebrać połączenia przychodzące w celu słuchania dźwięków otoczenia. • Oprogramowanie powinno udostępniać kamerę i mikrofon w celu rejestracji w przypadku kradzieży urządzenia. • Oprogramowanie powinno informować o poziomie bezpieczeństwa urządzenia, w graficzny sposób. • Oprogramowanie powinno automatycznie i regularnie aktualizować. • Oprogramowanie powinno pozwalać na stworzenie listy zaufanych kart SIM do 50 różnych kart. • Oprogramowanie powinno w przypadku dwóch nieudanych prób wprowadzenia hasła blokady ekranu, wykonać automatycznie zdjęcie przy	

		wykorzystaniu aparatu na froncie i tyle urządzenia. • Oprogramowanie powinno posiadać skróty do ustawień WiFI, Bluethoot, Przesyłanei danych pakietowych. • Oprogramowanie powinno posiadać certyfikaty AVTest oraz AV Comparatives Approved mobile produkt. • konto w chmurze o pojemności 1GB • Zdalne blokowanie/odblokowywanie telefonu przez sms • Zdalne usuwanie danych prywatnych kontakty, sms, zdarzenia w kalendarzu oraz pamiec zewnetrzna i wewnetrzna przy wykożystaniu SMS • Zdalne wywołanie automatycznego odbioru w celu nasłuchu otoczenia wyzwalane sms • Zdalne wyzwolenie nagrywania audio i video zapisywane w chmurze wyzwalanej z sms • Zdalne wywołanie połączeni zwrotnego w celu nasłuchu otoczenia wyzwalane przez sms • Blokowanie Stron Internetowych z podziałem na kategorie • Wykluczenia z filtra zadanych adresów URL • Obsługa następujących przeglądarek Firefox Maxthon Opera & Opera Mini Web Browser & Explorer Next APUS Yolo • Zarządzenie ilością przesyłanych danych pakietowych musi być możliwe na telefonach dual-SIM z tworzeniem polityki na konkretną kartę sim • Tryb blokowania urządzenia jeżeli włączony jest tryb samolotowy • Jeżeli urządzenie jest zablokowanie żadne wiadomości i informacje nie będą wyświetlane na ekranie urządzenia.	

		• Oprogramowanie musi w przypadku zgubienia kodu PIN, mieć możliwość uwierzytelnienia się przez zaufane konto Google i pozwolić na konfigurację w tym celu połączenia wifi. • Producent oprogramowania musi mieć dział wsparcia dostępny po chat oraz www. • Blokowanie grup numerów telefonów zaczynających się od (dane zdefiniowane przez użytkownika np.: 0700) • Oprogramowanie powinno pozwalać na wybranie do jakich danych prywatnych może mogą mieć dostęp aplikacje producentów trzecich np.: nr kart kredytowych, kontakty itp. • Okno pokazujące: zużycie RAM. Możliwość wyłączenia działających w tle aplikacji, • Po nagromadzeniu się ponad 10 wiadomości w folderze SPAM - wyświetli się informacja przez 7 dni na ekranie codziennie o 9.00 rano. • Śledzi zużycie baterii • Drugie wprowadzenie błędnego hasło do aplikacji powoduje zrobienie zdjęcia • konto w chmurze o pojemności 1GB • Blokowanie kodem PIN przed wglądem do kontaktów aplikacji, dokumentów galerii zdjęć i video, z możliwością wyboru pojedynczego elementu	