Centrum Usług Wspólnych
Powiatu Kętrzyńskiego
Pl. Grunwaldzki 1
11-400 Kętrzyn

Kętrzyn, dnia 23.08.2018 r.

Wykonawcy
biorący udział w postępowaniu
nr CUW.PK.343.35.2018

CUW.PK.343.35.2018

Dot.: postępowania o udzielenie zamówienia publicznego nr CUW.PK.343.35.2018 w trybie przetargu nieograniczonego pt: „Rozbudowa systemu obsługi informatycznej procesów związanych z funkcjonowaniem Centrum Usług Wspólnych Powiatu Kętrzyńskiego oraz jednostek organizacyjnych przez niego obsługiwanych *w ramach projektu: Wdrożenie e-usług w Centrum Usług Wspólnych Powiatu Kętrzyńskiego oraz jednostkach organizacyjnych przez niego obsługiwanych finansowana ze środków Europejskiego Funduszu Rozwoju Regionalnego (EFRR) w ramach Regionalnego Programu Operacyjnego Województwa Warmińsko-Mazurskiego na lata 2014-2020- Oś priorytetowa 3 Cyfrowy Region Działanie 3.1 Cyfrowa dostępność informacji sektora publicznego oraz wysoka, jakość e- usług publicznych".*

MODYFIKACJA SIWZ - NR 2

Centrum Usług Wspólnych Powiatu Kętrzyńskiego, działając w imieniu Zamawiającego w oparciu o pełnomocnictwo z dnia 18.07.2018 r. udzielone przez Zarząd Powiatu w Kętrzynie w trybie art. 15 i 18 ustawy z dnia 29 stycznia 2004 r. - Prawo zamówień publicznych (t.jedn. Dz.U. z 2017r. poz. 1579 z późn. zm.), w postępowaniu o udzielenie zamówienia publicznego nr CUW.PK.343.35.2018 w trybie przetargu nieograniczonego pt.: **„Rozbudowa systemu obsługi informatycznej procesów związanych z funkcjonowaniem Centrum Usług Wspólnych Powiatu Kętrzyńskiego oraz jednostek organizacyjnych przez niego obsługiwanych** *w ramach projektu:* ***Wdrożenie e-usług w Centrum Usług Wspólnych Powiatu Kętrzyńskiego oraz jednostkach organizacyjnych przez niego obsługiwanych*** *finansowana ze środków Europejskiego Funduszu Rozwoju Regionalnego (EFRR) w ramach Regionalnego Programu Operacyjnego Województwa Warmińsko-Mazurskiego na lata 2014-2020- Oś priorytetowa 3 Cyfrowy Region Działanie 3.1 Cyfrowa dostępność informacji sektora publicznego oraz wysoka, jakość e- usług publicznych***"**, na podstawie art. 38 ust. 4 ustawy Prawo Zamówień Publicznych wprowadza modyfikację specyfikacji istotnych warunków zamówienia w następującym zakresie:

1. Rozdział V ust. 3 pkt b ppkt 2). SIWZ otrzymuje następujące brzmienie:

Przed modyfikacją:	**Po modyfikacji:**
2) **2 zadania**, każde o wartości **min. 300.000** brutto, którego przedmiotem było: dostawa i konfiguracja środowiska witalizacyjnego oraz systemu archiwizacji danych; dostawa i wdrożenie oprogramowania wspierającego procesy dydaktyczne w placówkach oświatowych wraz z wdrożeniem platformy świadczenia e-usług publicznych.	2) **2 zadania**, każde o wartości **min. 300.000** brutto, którego przedmiotem było: dostawa i konfiguracja środowiska witalizacyjnego ~~oraz systemu archiwizacji danych~~; dostawa i wdrożenie oprogramowania wspierającego procesy dydaktyczne w placówkach oświatowych wraz z wdrożeniem platformy świadczenia e-usług publicznych.

2. W związku z powyższą zmianą modyfikuje się Zał. Nr 7 do SIWZ – w stopce załącznika zmienia się zapisy w nawiasie:

Przed modyfikacją:	**Po modyfikacji:**
*(Należy wykazać wykonanie minimum **2 zadania**, każde o wartości **min. 900.000** brutto, którego przedmiotem były: dostawa sprzętu komputerowego PC; dostawa i konfiguracja środowiska przetwarzania danych – serwery, macierze; oraz **2 zadania**, każde o wartości **min. 300.000** brutto, którego przedmiotem było: dostawa i konfiguracja środowiska witalizacyjnego oraz systemu archiwizacji danych; dostawa i wdrożenie oprogramowania wspierającego procesy dydaktyczne w placówkach oświatowych wraz z wdrożeniem platformy świadczenia e-usług publicznych.)*	*(Należy wykazać wykonanie minimum **2 zadania**, każde o wartości **min. 900.000** brutto, którego przedmiotem były: dostawa sprzętu komputerowego PC; dostawa i konfiguracja środowiska przetwarzania danych – serwery, macierze; oraz **2 zadania**, każde o wartości **min. 300.000** brutto, którego przedmiotem było: dostawa i konfiguracja środowiska witalizacyjnego ~~oraz systemu archiwizacji danych~~; dostawa i wdrożenie oprogramowania wspierającego procesy dydaktyczne w placówkach oświatowych wraz z wdrożeniem platformy świadczenia e-usług publicznych.)*

3. w zał. nr 5 do SIWZ – Opis przedmiotu zamówienia, sekcja „5.2 Wymagania ogólne obligatoryjne", na końcu tabeli w rozdz. 5.2. dodaje się zapis:

29.	Zamawiający dopuści realizację dostępu do narzędzi komunikacyjnych typu Skype na infrastrukturze usługodawcy

4. w zał. nr 5 do SIWZ – Opis przedmiotu zamówienia, sekcja „5.5 e-Usługi", opis pkt. 5.5.3. „**e-Powiadomienia**" tabela otrzymuje brzmienie:

Przed modyfikacją:

L.p.	Treść wymagania
1.	**Funkcjonalności:**
	możliwość tekstowej komunikacji dwustronnej szkoła/rodzice/uczniowie oraz za pośrednictwem modułu OSIN dla Organu Prowadzącego, komunikacja Urząd/szkoła/rodzice/uczniowie);
	możliwość uzyskiwania przez rodziców/Uczniów automatycznych powiadomień (poprzez dedykowane aplikacje mobilne) dotyczących istotnych dla nich zdarzeń: np. nieobecności dziecka w szkole, postępów w nauce i innych;
	dzięki odpowiednio skonstruowanym mechanizmom autoryzacji każdego użytkownika, po dokonaniu niezbędnych zmian w dokumentacji szkolnej istnieje możliwość stosowania systemu jako narzędzia do wiążącego doręczania informacji (np. dotyczących usprawiedliwiania nieobecności, informowania o wynikach klasyfikacji i innych, w zakresie zależnym tylko od woli szkoły);
2.	**Zadania:**
	Unowocześnienie i usprawnienie komunikacji i obiegu wybranych dokumentów pomiędzy organem prowadzącym a szkołami
	Zapewnienie aktualnego i wiarygodnego dostępu do najbardziej potrzebnych zestawień, statystyk i porównań.
3.	**Poziom dojrzałości: 4 - transakcja**
4.	**Typ usługi: A2C**

Po modyfikacji:

L.p.	Treść wymagania
1.	**Funkcjonalności:**
	~~możliwość tekstowej komunikacji dwustronnej szkoła/rodzice/uczniowie oraz za pośrednictwem modułu OSIN dla Organu Prowadzącego, komunikacja Urząd/szkoła/rodzice/uczniowie);~~ wykreślono
	możliwość uzyskiwania przez rodziców/Uczniów automatycznych powiadomień (poprzez dedykowane aplikacje mobilne) dotyczących istotnych dla nich zdarzeń: np. nieobecności dziecka w szkole, postępów w nauce i innych;
	dzięki odpowiednio skonstruowanym mechanizmom autoryzacji każdego użytkownika, po dokonaniu niezbędnych zmian w dokumentacji szkolnej istnieje możliwość stosowania systemu jako narzędzia do wiążącego doręczania informacji (np. dotyczących usprawiedliwiania nieobecności, informowania o wynikach klasyfikacji i innych, w zakresie zależnym tylko od woli szkoły);
2.	**Zadania:**
	Unowocześnienie i usprawnienie komunikacji i obiegu wybranych dokumentów pomiędzy organem prowadzącym a szkołami
	Zapewnienie aktualnego i wiarygodnego dostępu do najbardziej potrzebnych zestawień, statystyk i porównań.
3.	**Poziom dojrzałości: 4 - transakcja**
4.	**Typ usługi: A2C**

5. w zał. nr 5 do SIWZ – Opis przedmiotu zamówienia, sekcja „5.5 e-Usługi", opis pkt. 5.5.7. „**e-Dydaktyka**" tabela otrzymuje brzmienie:

Przed modyfikacją:

L.p.	Treść wymagania
1.	**Funkcjonalności:**
	Przypisywanie umiejętności z podstawy programowej do tematu z rozkładu materiału nauczania.
	Zliczanie zrealizowanych godzin z każdego przedmiotu na danym etapie edukacyjnym.
2.	**Zadania:**
	Unowocześnienie i usprawnienie komunikacji i obiegu wybranych dokumentów pomiędzy organem prowadzącym a szkołami
	Usprawnienie planowania przebiegu lekcji – raz przypisane do tematu materiały i notatki widoczne są dla nauczyciela podczas tych samych zajęć w innych klasach.
3.	**Poziom dojrzałości: 3 - interakcja dwustronna**
4.	**Typ usługi: A2C**

Po modyfikacji:

L.p.	Treść wymagania
1	**Funkcjonalności:**
	Przypisywanie umiejętności z podstawy programowej do tematu z rozkładu materiału nauczania.
	Zliczanie zrealizowanych godzin z każdego przedmiotu na danym etapie edukacyjnym.
2.	**Zadania:**
	Unowocześnienie i usprawnienie komunikacji i obiegu wybranych dokumentów pomiędzy organem prowadzącym a szkołami
	Usprawnienie planowania przebiegu lekcji – raz przypisane do tematu materiały i notatki widoczne są dla nauczyciela podczas tych samych zajęć w innych klasach.
3.	**Poziom dojrzałości: 3 - interakcja dwustronna**
4.	**Typ usługi: A2C**

6. w zał. nr 5 do SIWZ – Opis przedmiotu zamówienia, sekcja „5.5 e-Usługi", opis pkt. 5.5.8. „**e-Dokumentacja**" tabela otrzymuje brzmienie:

Przed modyfikacją:

L.p.	Treść wymagania
1.	**Funkcjonalności:**
	Przypisywanie umiejętności z podstawy programowej do tematu z rozkładu materiału nauczania.
	Zliczanie zrealizowanych godzin z każdego przedmiotu na danym etapie edukacyjnym.
2.	**Zadania:**
	Unowocześnienie i usprawnienie komunikacji i obiegu wybranych dokumentów pomiędzy organem prowadzącym a szkołami
	Usprawnienie planowania przebiegu lekcji – raz przypisane do tematu materiały i notatki widoczne są dla nauczyciela podczas tych samych zajęć w innych klasach.
3.	**Poziom dojrzałości: 3 - interakcja dwustronna**
4.	**Typ usługi: A2C**

Po modyfikacji:

L.p.	Treść wymagania
1	**Funkcjonalności:**
	Monitorowanie postępów w realizowaniu programu w danej klasie lub przez określonego nauczyciela
	Sprawdzanie brakującej lub ponadwymiarowej frekwencji uczniów
	Odnotowywanie szczegółów dotyczących dodatkowych godzin nauczycieli czy realizowania przez nich nauczania indywidualnego
2.	**Zadania:**
	Dokumentowanie pracy placówki edukacyjnej.
	Prowadzenie dokumentacji przebiegu nauczania wyłącznie w formie elektronicznej
3.	**Poziom dojrzałości: 3 – nie dotyczy**
4.	**Typ usługi: A2A**

7. w zał. nr 5 do SIWZ – Opis przedmiotu zamówienia, sekcja „5.5 e-Usługi", opis pkt. 5.5.12. Wymagania niefunkcjonalne po tabeli dodaje się zapis:

Zamawiający odstąpi od konieczności realizacji wymagania 5.5.12. dla wszystkich aplikacji i uzna dostarczenie dedykowanych aplikacji mobilnych za spełnienie wymagania.

8. w zał. nr 5 do SIWZ – Opis przedmiotu zamówienia, sekcja „5.9 Modernizacja środowiska serwerowego", opis dla „**Serwer aplikacyjny SA1 -SA14 - 14 szt.**" po tabeli z opisem dodaje się zapisy:

Lub serwery aplikacyjny SA1 -SA14 zgodne ze specyfikacją:

Lp	Parametr lub warunek	Minimalne wymagania
1	**Obudowa**	Obudowa typu wieża z możliwością instalacji w szafie RACK 19", wysokości maksymalnie 5U. Wraz z serwerem mają zostać dostarczone wszystkie niezbędne elementy to instalacji w szafie rack.
2	**Płyta główna**	-Dwuprocesorowa, wyprodukowana i zaprojektowana przez producenta serwera, - Możliwość instalacji 2 procesorów; - Minimum 6 złącz PCI Express generacji 3, w tym minimum 1 złącza o prędkości x16 i 3 złącza o prędkości x8; - Wszystkie złącza PCI Express muszą być aktywne; - Minimum 2 sloty dla dysków M.2 na płycie głównej (lub dedykowanej karcie PCI

		Express) nie zajmujące klatek dla dysków hot-plug; (Możliwość integracji dedykowanej, wewnętrznej pamięci flash przeznaczonej dla wirtualizatora w slocie M.2 bez zajmowania klatek dyskowych serwera);
3	**Procesory**	- Obsługa procesorów minimum 24-rdzeniowych; mocy do min. 150W i taktowaniu do min.3.6GHz -Zainstalowane minimum jeden procesor 4-rdzeniowy osiągający w testach PassMark – CPU Mark wynik nie gorszy niż 8600 punktów. Wynik testu musi być opublikowany na stronie www.cpubenchmark.net
4	Pamięć RAM	-Zainstalowane 16 GB pamięci RAM typu DDR4 Registered, 2666Mhz -Wsparcie dla technologii zabezpieczania pamięci Advanced ECC, SDDC; -Minimum 12 gniazda pamięci RAM na płycie głównej, obsługa minimum 512GB pamięci RAM
5	Kontrolery dyskowe, I/O	-Zainstalowany kontroler SAS 3.0 RAID 0,1,5,6,50,60 2GB pamięci podręcznej cache, -Wyposażony w nieulotną pamięć cache o pojemności min. 2GB; - Możliwość zainstalowania kontrolera SAS 3.0 RAID 0,1,5,6,50,60 wyposażonego w co najmniej 4 GB pamięci cache
6	Dyski twarde	- Zainstalowane 2 dyski SDD minimum 240GB typu Read Intensive - Zainstalowane 2 dyski HDD SATA o pojemności minimum 1TB i prędkości obrotowej min 7200 obrotów - Minimum 8 wnęk dla dysków twardych Hotplug 2,5, z możliwością rozbudowy do 16 wnęk 2,5" - Możliwość zainstalowania 2 nośników Flash w o pojemności co najmniej 64GB przeznaczonej dla wirtualizatora
7	Inne napędy zintegrowane	Możliwość instalacji wewnętrznego napędu DVD-RW
8	Kontrolery LAN	-Jedna dwuportowa karta 2x1Gbit/s ze wsparciem iSCSI, niezajmująca slotu PCI Express;
10	Porty	-zintegrowana karta graficzna ze złączem VGA; - minimum 2x USB 3.0 dostępne na froncie obudowy - minimum 2x USB 3.0 dostępne z tyłu serwera - minimum 2x USB wewnątrz serwera Ilość dostępnych złącz VGA i USB nie może być osiągnięta poprzez stosowanie zewnętrznych przejściówek, rozgałęziaczy czy dodatkowych kart rozszerzeń zajmujących jakikolwiek slot PCI Express serwera;
11	Zasilanie, chłodzenie	- Redundantne zasilacze hotplug o mocy minimum 450W, o sprawności 94% (tzw klasa Platinum) - Redundantne wentylatory hotplug; - Możliwość skonfigurowania serwera do pracy w temperaturze otoczenia równej 45st.C,
12	Zarządzanie	-Wbudowane diody informacyjne informujące o stanie serwera; -Zintegrowany z płytą główną serwera kontroler sprzętowy zdalnego zarządzania zgodny z IPMI 2.0 o funkcjonalnościach: • Niezależny od systemu operacyjnego, sprzętowy kontroler umożliwiający pełne zarządzanie, zdalny restart serwera; • Dedykowana karta LAN 1 Gb/s (dedykowane złącze RJ-45 z tyłu obudowy) do komunikacji wyłącznie z kontrolerem zdalnego zarządzania z możliwością przeniesienia tej komunikacji na inną kartę sieciową współdzieloną z systemem operacyjnym; • Dostęp poprzez przeglądarkę Web (także SSL, SSH) • Zarządzanie mocą i jej zużyciem oraz monitoring zużycia energii • Zarządzanie alarmami (zdarzenia poprzez SNMP) • Możliwość przejęcia konsoli tekstowej • Przekierowanie konsoli graficznej na poziomie sprzętowym oraz możliwość montowania zdalnych napędów i ich obrazów na poziomie sprzętowym (cyfrowy KVM) • Sprzętowy monitoring serwera w tym stanu dysków twardych i kontrolera RAID (bez pośrednictwa agentów systemowych) • Karta zarządzająca musi sprzętowo wspierać wirtualizację warstwy sieciowej serwera, bez wykorzystania zewnętrznego hardware - wirtualizacja MAC i WWN na wybranych kartach zainstalowanych w serwerze (co najmniej wsparcie dla technologii kart 10Gbit/s Ethernet i kart FC 8Gbit/s oferowanych przez producenta serwera) • Oprogramowanie zarządzające i diagnostyczne wyprodukowane przez producenta serwera umożliwiające konfigurację kontrolera RAID, instalację systemów operacyjnych, zdalne zarządzanie, diagnostykę i przewidywanie awarii w oparciu o informacje dostarczane w ramach zintegrowanego w serwerze systemu umożliwiającego monitoring systemu i środowiska (m.in. temperatura, dyski, zasilacze, płyta główna, procesory, pamięć operacyjna itd.).

13	Wspierane OS	- Windows 2016 Hyper-V, Windows 2012 R2 Hyper-V, VMWare, Suse, RHEL
14	Gwarancja	-3 lata gwarancji producenta serwera w trybie onsite -Dostępność części zamiennych przez 5 lat od momentu zakupu serwera; -Wymagana jest bezpłatna dostępność poprawek i aktualizacji BIOS/Firmware/sterowników dożywotnio dla oferowanego serwera – jeżeli funkcjonalność ta wymaga dodatkowego serwisu lub licencji producenta serwera takowa licencja musi być uwzględniona w konfiguracji;
15	Dokumentacja, inne	-Elementy, z których zbudowane są serwery muszą być produktami producenta tych serwerów lub być przez niego certyfikowane oraz całe muszą być objęte gwarancją producenta, o wymaganym w specyfikacji poziomie SLA (wymagane oświadczenie producenta serwera potwierdzające spełnienie wymagań dołączone do oferty). -Serwer musi być fabrycznie nowy i pochodzić z oficjalnego kanału dystrybucyjnego w Polsce - Wymagane oświadczenie producenta serwera, że oferowany do przetargu sprzęt spełnia ten wymóg; -Oferent zobowiązany jest dostarczyć wraz z ofertą kartę produktową oferowanego serwera umożliwiającą weryfikację parametrów oferowanego sprzętu; -Ogólnopolska, telefoniczna infolinia/linia techniczna producenta serwera, (ogólnopolski numer o zredukowanej odpłatności 0-800/0-801, w ofercie należy podać nr telefonu) w czasie obowiązywania gwarancji na sprzęt i umożliwiająca po podaniu numeru seryjnego urządzenia weryfikację: konfiguracji sprzętowej serwera, w tym model i typ dysków twardych, procesora, ilość fabrycznie zainstalowanej pamięci operacyjnej, czasu obowiązywania i typ udzielonej gwarancji; -Możliwość aktualizacji i pobrania sterowników do oferowanego modelu serwera w najnowszych certyfikowanych wersjach bezpośrednio z sieci Internet za pośrednictwem strony www producenta serwera;

9. w zał. nr 5 do SIWZ – Opis przedmiotu zamówienia, sekcja „5.9 Modernizacja środowiska serwerowego", opis dla „**Serwerowy system operacyjny**" po tabeli z opisem wymagań minimalnych dodaje się zapisy:

LUB ROZWIĄZANIE Serwerowy system operacyjny:

- Oprogramowanie dostępne na licencji GPL lub równoważnej, która będzie pozwalała na audyt kodu źródłowego oferowanego rozwiązania,
- Zarządzanie systemem wirtualizacji jest realizowane za pomocą dedykowanej konsoli dostępnej z poziomu przeglądarki internetowej lub uruchamianej bezpośrednio w systemie operacyjnym
- System operacyjny posiada wbudowany mechanizm wirtualizacji z możliwością uruchamia nielimitowanej ilości maszyn wirtualnych,
- System operacyjny posiada wbudowany mechanizm bezpieczeństwa RBAC (SELinux lub AppArmor),
- System operacyjny posiada wbudowany mechanizm filtrowania pakietów z możliwością przydzielania wybranych interfejsów sieciowych do wskazanych stref,
- Oferowany system operacyjny umożliwia instalowanie i zarządzanie oprogramowaniem, które będzie na nim uruchamiane, w postaci gotowych standardowych pakietów oprogramowania,
- Oferowany system operacyjny posiada wbudowany mechanizm ograniczania zasobów systemowych dla wskazanych procesów lub grup procesów,
- System operacyjny umożliwia dostosowanie parametrów jego instalacji i automatyzację instalacji poprzez takie mechanizmy jak Kickstart lub AutoYaST,
- Oferowany system operacyjny jest zgodny z jednym następujących mechanizmów automatyzujących zadania administracyjne: Salt, Puppet Lub Ansible,
- System operacyjny oferuje funkcjonalność „Domeny Windows" do podłączenia klientów z systemami operacyjnymi Microsoft Windows realizowaną w postaci funkcjonalności wbudowanej w system operacyjny lub gotowego rozwiązania uruchamianego na nim w postaci wirtualnej maszyny,
- Oferowany system operacyjny jest w pełni zgodny z oferowaną w niniejszym postępowaniu Platformą Wirtualizacyjną,
- Oferowany system operacyjny posiada wsparcie techniczne producenta, dostępne w języku polskim, oferowane w trybie 24h dostępne za pomocą jednej z wymienionych metod: poczta elektroniczne lub telefon, z nieograniczoną ilością zgłoszeń.

10. w zał. nr 5 do SIWZ – Opis przedmiotu zamówienia, sekcja „5.9 Modernizacja środowiska serwerowego", opis dla „**Platforma wirtualizacyjna– 1 kpl. - obejmująca serwery S1 i S2**" po tabeli z opisem wymagań minimalnych dodaje się zapisy:

LUB ROZWIĄZANIE Platforma wirtualizacyjna:

- Oprogramowanie jest dostępne na licencje GPL lub równoważnej, która będzie pozwalała na audyt kodu źródłowego oferowanego rozwiązania,

- Zarządzanie systemem wirtualizacji musi być realizowane za pomocą konsoli dostępnej z poziomu przeglądarki internetowej,
- Wirtualizator oferowanej platformy działa w systemie operacyjnym z działającym mechanizmem bezpieczeństwa RBAC (SELinux lub AppArmor),
- Konsola zarządzająca oferowaną platformą wirtualizacyjną umożliwia instalację na fizycznym serwerze oraz jako appliance maszyny wirtualnej uruchamianej bezpośrednio na platformie wirtualizacyjnej,
- Oprogramowanie umożliwia uruchamianie następujących systemów operacyjnych: Red Hat Enterprise Linux 5,6 (32 i 64 bity) oraz 7 (64 bity), Microsoft Windows Serwer 2008, 2008r2, 2012 (32 i 64 bity) oraz 2016, SUSE Linux Enterprise Server 10, 11 i 12, Debian w wersji 9,
- platforma wirtualizacyjna musi zapewniać mechanizmy wysokiej dostępności dla uruchamianych maszyn wirtualnych (HA),
- Oferowana platforma wirtualizacyjna posiada wsparcie dla technologii Nvidia vGPU,
- Oferowana platforma wirtualizacyjna oferuje mechanizm migracji typu V2V dla systemów Debian, Windows i Red Hat Enterpise Linux
- W systemie wirtualizacji, w panelu administracyjnym, istnieje możliwość definiowania:
  - wzorców wirtualnych maszyn,
  - zdefiniowanych zasobów systemowych (instalacja w oparciu o typ instancji),
  - ról systemowych dla użytkowników,
- Oprogramowanie umożliwia wykonywania kopii migawkowych (ang. snapshot) uruchamianych wirtualnych maszyn,
- Oprogramowanie działa w oparciu o wirtualizator KVM,
- Oprogramowanie umożliwia definiowanie różnych typów sieci logicznych,
- Oprogramowanie oferuje wsparcie dla sieci definiowanych programowo (ang. SDN)
- Oprogramowanie udostępnia interfejs programistyczny (API) oraz obsługiwać protokół SNMP do monitorowania środowiska,
- Oprogramowanie umożliwia podłączenie do usługi katalogowej LDAPv3
- Oprogramowanie posiada możliwość wykorzystywania następujących protokołów dostępowych do zasobów dyskowych:
  - iSCSI
  - Fiber Channel
  - NFS
  - GlusterFS
  - Ceph (realizowany za pomocą CephFS lub RBD lub iSCSI Gateway)
  - lokalny zasób dyskowy zgodny ze standardem POSIX
- Oferowane oprogramowanie posiada wsparcie techniczne producenta, dostępne w języku polskim, oferowane w trybie 24h dostępne za pomocą jednej z wymienionych metod: poczta elektroniczna lub telefon, z nieograniczoną ilością zgłoszeń.

11. w zał. nr 5 do SIWZ – Opis przedmiotu zamówienia, sekcja „5.9 Modernizacja środowiska serwerowego", opis dla „**Oprogramowanie do backupu środowisk wirtualnych – obejmujące serwery S1 i S2**" po tabeli z opisem wymagań minimalnych dodaje się zapisy:

LUB ROZWIĄZANIE **Oprogramowanie do backupu środowisk wirtualnych**:

- Oprogramowanie działa w architekturze klient – serwer
- Oprogramowanie posiada konsolę administracyjną dostępną z poziomu linii poleceń jak również poprzez przeglądarkę internetową
- serwer kopii zapasowych działa na jednej ze wskazanych dystrybucji Linux: Red Hat Enterprise Linux 7, SUSE Enterprise Linux 12, CentOS 7 lub OpenSUSE 42.3
- umożliwia wykonywanie kopii zapasowych w modelach: backup to tape, backup to disk oraz backup to disk to tape
- wykorzystuje szyfrowany protokół transmisji w komunikacji pomiędzy serwerem a klientem
- umożliwia tworzenie skryptów uruchamianych przed i po zadaniu tworzenia kopii zapasowej
- umożliwia tworzenie kopii zapasowych pełnych, przyrostowych i różnicowych
- wykorzystuje harmonogram do automatycznego uruchamiania zadań tworzenia kopii zapasowych
- umożliwia szyfrowanie taśm LTO
- po stronie klienta obsługuje w trybie dostępu plikowego systemy operacyjne Linux, Windows orac MacOS
- posiada wsparcie dla środowiska wirtualizacyjnego VMWare oraz KVM
- posiada wsparcie dla protokołu NDMP
- po stronie serwera obsługiwane są pojedyncze napędy taśmowe jak również zmieniarki napędów taśmowych z obsługą kodów kreskowych
- oprogramowanie przechowuje informacje z działania systemu tworzenia kopii zapasowych (catalog) w jednej z następujących baz danych typu Open Source: PostgreSQL, MySQL / MariaDB lub SQLite

oprogramowanie obsługuje rozwiązania typu SDS jako miejsce przechowywania danych: GlusterFS oraz Ceph.

12. w zał. nr 5 do SIWZ – Opis przedmiotu zamówienia, sekcja „5.10 Modernizacja inforstruktury teletechnicznej", opis dla **„Kontroler sieci Wi-Fi – centralny system do zarządzania punktami dostępowymi w układzie sieci rozproszonych w 6 lokalizacjach Zamawiającego– 1 szt."** po tabeli z opisem wymagań minimalnych dodaje się zapisy:

Zamawiający dopuszcza zaoferowanie centralnego kontrolera sieci WIFI, z wszystkimi wyspecyfikowanymi parametrami w postaci usługi w chmurze producenta rozwiązania z pięcioletnim okresem wsparcia.

13. w zał. nr 5 do SIWZ – Opis przedmiotu zamówienia, sekcja „5.10 Modernizacja inforstruktury teletechnicznej", opis dla **„Punkt dostępowy (AP) sieci bezprzewodowej Wi-Fi - 34 szt."** wiersz 3 otrzymuje brzmienie:

Przed modyfikacją:

3.	Funkcjonalności, normy techniczne	1. Punkt dostępowy musi mieć możliwość współpracy z centralnym kontrolerem sieci bezprzewodowej 2. Punkt dostępowy musi mieć możliwość pracy w trybie autonomicznym tj. bez nadzoru centralnego kontrolera: a. Punkt dostępowy musi posiadać funkcjonalność zarządzania przez przeglądarkę internetową i protokół https b. Wszystkie operacje konfiguracyjne muszą być możliwe do przeprowadzenia z poziomu przeglądarki c. Przełączenie punktu dostępowego do pracy z centralnym kontrolerem może odbywać się tylko poprzez zmianę ustawienia trybu pracy urządzenia z poziomu GUI. Zmiana trybu pracy nie może się odbywać poprzez instalację na urządzeniu, nowej wersji oprogramowania. 3. Musi być zapewniona możliwość wspólnej konfiguracji punktów połączonych w jedną sieć LAN w warstwie 2: a. System operacyjny zainstalowany w punktach dostępowych musi umożliwiać automatyczny wybór jednego punktu dostępowego jako elementu zarządzającego b. W przypadku awarii punktu zarządzającego kolejny punkt dostępowy w sieci musi przejąć jego rolę w sposób automatyczny c. Modyfikacja konfiguracji musi się automatycznie propagować na pozostałe punkty dostępowe d. Obraz systemu operacyjnego musi się automatycznie propagować na pozostałe punkty dostępowe, aby wszystkie punkty miały tą samą jego wersję e. Tworzenie klastra złożonego co najmniej z 120 urządzeń 4. Punkt dostępowy musi mieć możliwość pracy w trybie monitorującym pasmo radiowe w celu wykrywania np. fałszywych AP 5. Punkt dostępowy musi posiadać wbudowany moduł pozwalający na bezpieczne przechowywanie poświadczeń i kluczy 6. Punkt dostępowy musi obsługiwać nie mniej niż 16 niezależnych SSID na radio 7. Punkt dostępowy musi obsługiwać minimum 255 użytkowników na radio 8. Każde SSID musi mieć możliwość przypisania w sposób statyczny lub dynamiczny do sieci VLAN 9. Zarządzanie pasmem radiowym w sieci punktów dostępowych musi się odbywać automatycznie za pomocą auto-adaptacyjnych mechanizmów, w tym nie mniej niż: a. Automatyczne definiowanie kanału pracy oraz mocy sygnału dla poszczególnych punktów dostępowych przy uwzględnieniu warunków oraz otoczenia, w którym pracują punkty dostępowe b. Stałe monitorowanie pasma oraz usług w celu zapewnienia niezakłóconej pracy systemu c. Rozkład ruchu pomiędzy różnymi punkami dostępowym oraz pasmami bazując na ilości użytkowników oraz utylizacji pasma d. Wykrywanie interferencji oraz miejsc bez pokrycia sygnału e. Automatyczne przekierowywanie klientów, którzy mogą pracować w pasmie 5GHz f. Wyrównywanie czasów dostępu do pasma dla klientów

		pracujących w standardzie 802.11n/ac oraz starszych (802.11b/g) 10. Minimalizacja interferencji związanych z sieciami 3G/4G LTE 11. Punkt dostępowy musi posiadać minimum 2 wbudowane anteny dwuzakresowe pracujące w trybie 2x2 MIMO, z parametrami co najmniej: 3.2dBi dla 2,4GHz, 6.2 dBi dla 5GHz 12. Obsługa standardów 802.11a, 802.11b, 802.11g, 802.11n, 802.11ac 1 Wave 13. Specyfikacja radia 802.11a/n/ac: a. Obsługiwanatechnologia OFDM b. Typy modulacji: BPSK, QPSK, 16-QAM, 64-QAM, 256-QAM c. Moc transmisji konfigurowalna przez administratora – możliwość zmiany co 0.5dbm d. Prędkości transmisji: • 6, 9, 12, 18, 24, 36, 48, 54 Mbps dla 802.11a, • 6,5Mbps do 400Mbps dla 802.11n • 6.5 Mbps do 867 Mbps dla 802.11ac e. Obsługa HT – kanały 20/40MHz dla 802.11n f. Obsługa VHT – kanały 20/40/80MHz dla 802.11ac g. Wsparcie dla technologii DFS (Dynamicfrequencyselection) – dla wszystkich 80Mhz kanałów w paśmie 5GHz h. Agregacja pakietów: A-MPDU, A-MSDU dla standardów 802.11n/ac i. Wsparciedla: • MRC (Maximal ratio combining) • CDD/CSD (Cyclic delay/shift diversity) • STBC (Space-time block coding) • LDPC (Low-density parity check) • TechnologiaTxBF 14. Specyfikacja radia 802.11b/g/n: a. Technologia direct sequence spread spectrum (DSSS), OFDM b. Typymodulacji – CCK, BPSK, QPSK,16-QAM, 64-QAM c. Moc transmisji konfigurowalna przez administratora d. Prędkości transmisji: • 1,2,5.5,11 Mbps dla 802.11b • 6,9,12,18,24,36,48,54 Mbps dla 802.11g 15. Punkt dostępowy musi posiadać co najmniej a. Co najmniej 1 interfejs 10/100/1000 Base-T • z funkcją auto-sensing link oraz MDI/MDX • z funkcją POE/POE+ • zgodny ze standardem 802.3az Energy Effcient Ethernet EEE b. interfejs konsoli c. interfejs Bluetooth Low Energy (BLE) d. przycisk przywracający konfigurację fabryczną e. slot zabezpieczający Keningston 16. Parametry pracy urządzenia: a. Temperatura otoczenia: 0-50 º C b. Wilgotność 5% - 95% c. Znak CE d. EN 300 328 e. EN 301 489 f. EN 301 893 g. EN 60601-1-1, EN60601-1-2 17. Punkt dostępowy zasilony przy użyciu zgodnym ze standardem 802.3af PoE nie może tracić, żadnej funkcjonalności dla radia pracującego w paśmie 5GHz w porównaniu do zasilenia go przy użyciu standardu 802.3at PoE+ 18. Pobór mocy nie większy niż 13W 19. Urządzenie musi posiadać certyfikat Wi-Fi Alliance (WFA) dla standardów 802.11/a/b/g/n/ac 20. Urządzenie musi być dostarczone z zestawem do montażu wewnątrz budynków (na ścianie)

Po modyfikacji:

3.	Funkcjonalności, normy techniczne	21. Punkt dostępowy musi mieć możliwość współpracy z centralnym kontrolerem sieci bezprzewodowej 22. Punkt dostępowy musi mieć możliwość pracy w trybie autonomicznym tj. bez nadzoru centralnego kontrolera: d. Punkt dostępowy musi posiadać funkcjonalność zarządzania przez przeglądarkę internetową i protokół https e. Wszystkie operacje konfiguracyjne muszą być możliwe do przeprowadzenia z poziomu przeglądarki f. Przełączenie punktu dostępowego do pracy z centralnym kontrolerem może odbywać się tylko poprzez zmianę ustawienia trybu pracy urządzenia z poziomu GUI. Zmiana trybu pracy nie może się odbywać poprzez instalację na urządzeniu, nowej wersji oprogramowania. 23. Musi być zapewniona możliwość wspólnej konfiguracji punktów połączonych w jedną sieć LAN w warstwie 2: a. System operacyjny zainstalowany w punktach dostępowych musi umożliwiać automatyczny wybór jednego punktu dostępowego jako elementu zarządzającego b. W przypadku awarii punktu zarządzającego kolejny punkt dostępowy w sieci musi przejąć jego rolę w sposób automatyczny c. Modyfikacja konfiguracji musi się automatycznie propagować na pozostałe punkty dostępowe d. Obraz systemu operacyjnego musi się automatycznie propagować na pozostałe punkty dostępowe, aby wszystkie punkty miały tą samą jego wersję e. Tworzenie klastra złożonego co najmniej z 120 urządzeń 24. Punkt dostępowy musi mieć możliwość pracy w trybie monitorującym pasmo radiowe w celu wykrywania np. fałszywych AP 25. Punkt dostępowy musi posiadać wbudowany moduł pozwalający na bezpieczne przechowywanie poświadczeń i kluczy 26. Punkt dostępowy musi obsługiwać nie mniej niż 16 niezależnych SSID na radio 27. Punkt dostępowy musi obsługiwać minimum 255 użytkowników na radio 28. Każde SSID musi mieć możliwość przypisania w sposób statyczny lub dynamiczny do sieci VLAN 29. Zarządzanie pasmem radiowym w sieci punktów dostępowych musi się odbywać automatycznie za pomocą auto-adaptacyjnych mechanizmów, w tym nie mniej niż: a. Automatyczne definiowanie kanału pracy oraz mocy sygnału dla poszczególnych punktów dostępowych przy uwzględnieniu warunków oraz otoczenia, w którym pracują punkty dostępowe b. Stałe monitorowanie pasma oraz usług w celu zapewnienia niezakłóconej pracy systemu c. Rozkład ruchu pomiędzy różnymi punkami dostępowym oraz pasmami bazując na ilości użytkowników oraz utylizacji pasma d. Wykrywanie interferencji oraz miejsc bez pokrycia sygnału e. Automatyczne przekierowywanie klientów, którzy mogą pracować w pasmie 5GHz f. Wyrównywanie czasów dostępu do pasma dla klientów pracujących w standardzie 802.11n/ac oraz starszych (802.11b/g) 30. Minimalizacja interferencji związanych z sieciami 3G/4G LTE 31. Punkt dostępowy musi posiadać minimum 2 wbudowane anteny dwuzakresowe pracujące w trybie 2x2 MIMO, z parametrami co najmniej: 3.2dBi dla 2,4GHz, 6.2 dBi dla 5GHz 32. Obsługa standardów 802.11a, 802.11b, 802.11g, 802.11n, 802.11ac 1 Wave

		33. Specyfikacja radia 802.11a/n/ac: a. Obsługiwanatechnologia OFDM b. Typy modulacji: BPSK, QPSK, 16-QAM, 64-QAM, 256-QAM c. Moc transmisji konfigurowalna przez administratora – możliwość zmiany co 0.5dbm d. Prędkości transmisji: • 6, 9, 12, 18, 24, 36, 48, 54 Mbps dla 802.11a, • 6,5Mbps do ~~400Mbps~~ 300Mbps dla 802.11n • 6.5 Mbps do 867 Mbps dla 802.11ac e. Obsługa HT – kanały 20/40MHz dla 802.11n f. Obsługa VHT – kanały 20/40/80MHz dla 802.11ac g. Wsparcie dla technologii DFS (Dynamicfrequencyselection) – dla wszystkich 80Mhz kanałów w paśmie 5GHz h. Agregacja pakietów: A-MPDU, A-MSDU dla standardów 802.11n/ac i. Wsparciedla: • MRC (Maximal ratio combining) • CDD/CSD (Cyclic delay/shift diversity) • STBC (Space-time block coding) • LDPC (Low-density parity check) • TechnologiaTxBF 34. Specyfikacja radia 802.11b/g/n: a. Technologia direct sequence spread spectrum (DSSS), OFDM b. Typymodulacji – CCK, BPSK, QPSK,16-QAM, 64-QAM c. Moc transmisji konfigurowalna przez administratora d. Prędkości transmisji: • 1,2,5.5,11 Mbps dla 802.11b • 6,9,12,18,24,36,48,54 Mbps dla 802.11g 35. Punkt dostępowy musi posiadać co najmniej a. Co najmniej 1 interfejs 10/100/1000 Base-T • z funkcją auto-sensing link oraz MDI/MDX • z funkcją POE/POE+ • zgodny ze standardem 802.3az Energy Effcient Ethernet EEE b. interfejs konsoli c. interfejs Bluetooth Low Energy (BLE) d. przycisk przywracający konfigurację fabryczną e. slot zabezpieczający Keningston 36. Parametry pracy urządzenia: a. Temperatura otoczenia: 0-50 º C b. Wilgotność 5% - 95% c. Znak CE d. EN 300 328 e. EN 301 489 f. EN 301 893 g. EN 60601-1-1, EN60601-1-2 37. Punkt dostępowy zasilony przy użyciu zgodnym ze standardem 802.3af PoE nie może tracić, żadnej funkcjonalności dla radia pracującego w paśmie 5GHz w porównaniu do zasilenia go przy użyciu standardu 802.3at PoE+ 38. Pobór mocy nie większy niż 13W 39. Urządzenie musi posiadać certyfikat Wi-Fi Alliance (WFA) dla standardów 802.11/a/b/g/n/ac 40. Urządzenie musi być dostarczone z zestawem do montażu wewnątrz budynków (na ścianie)

14. w zał. nr 5 do SIWZ – Opis przedmiotu zamówienia, sekcja „5.11 Zakup sprzętu i oprogramowania komputerowego", opis dla „**Komputer przenośny - 6 szt.**" wiersz 9 otrzymuje brzmienie:
Przed modyfikacją:

9	Bateria i zasilanie	Min. 6-ogniwowa [min. 96Whr]

Po modyfikacji:

9	Bateria i zasilanie	~~Min. 6-ogniwowa [min. 96Whr]~~ Bateria min. 56Wh

15. w zał. nr 5 do SIWZ – Opis przedmiotu zamówienia, sekcja „5.11 Zakup sprzętu i oprogramowania komputerowego", opis dla **„Oprogramowanie antywirusowe – 161 szt."** po tabeli z opisem wymagań minimalnych dodaje się zapisy:

LUB ROZWIĄZANIE Oprogramowanie antywirusowe:

1. Pełna obsługa systemów:
   - Windows XP SP3
   - Windows Vista SP2
   - Windows 7 SP1
   - Windows 8
   - Windows 8.1
   - Windows 10
   - Windows Server 2003 SP2
   - Windows Server 2003R2 SP2
   - Windows Server 2008 SP2
   - Windows Server 2008R2 SP1
   - Windows Server 2012
   - Windows Server 2012R2
   - Windows Server 2016
   - Android 4.4 lub nowszy
2. Pełne wsparcie dla systemów 32 bitowych i 64 bitowych.
3. Wspólny instalator pakietu dla systemów 32 bitowych i 64 bitowych kontrolujący niezbędne wymagania systemowe.
4. Interfejs programu dostępny w wersji polskiej i angielskiej z możliwością zmiany języka w trakcie pracy programu.
5. Wielopoziomowy silnik antywirusowy wykrywający wszystkie rodzaje zagrożeń:
   - konie trojańskie, wirusy, exploity, backdoory itp.
   - narzędzia hakerskie, aplikacje potencjalnie szkodliwe i niechciane.
   - aplikacje typu adware/spyware.
   - aplikacje ukrywające swoją obecność w systemie, rootkity.
6. Moduł pozwalający na pełne usunięcie wykrytych, niechcianych aplikacji łącznie z wykorzystywanymi przez nie bibliotekami, sterownikami i wpisami w rejestrze systemowym.
7. Skanowanie wszystkich popularnych formatów archiwów i konwerterów (w tym pakerów plików wykonywalnych).
8. Możliwość włączenia tzw. trybu gracza pozwalającego na pracę przy komputerze nie przerywaną ewentualnymi komunikatami programu - po włączeniu tego trybu program sam podejmuje decyzje w sytuacjach alarmowych.
9. Zaawansowane mechanizmy heurystyczne pozwalające na wykrywanie nieznanych jeszcze zagrożeń.
10. Możliwość indywidualnej zmiany ustawień poziomu heurystyki dla poszczególnych modułów ochronnych pakietu.
11. Dostęp do wszystkich wykrytych w systemie infekcji z poziomu głównego okna programu wraz z możliwością ich natychmiastowego usunięcia.
12. Zaawansowany skaner na żądanie.
13. Monitor antywirusowy kontrolujący wszystkie uruchamiane/otwierane/kopiowane/zapisywane pliki nie pozwalający na dostęp do plików zainfekowanych/szkodliwych.
14. Moduł kontroli rodzicielskiej/kontroli dostępu pozwalający na wszechstronne kontrolowanie/blokowanie treści pobieranych z Internetu.
15. Skaner poczty kontrolujący pocztę przesyłaną protokołami POP3/SMTP/IMAP.
16. Ochrona przeglądarki kontrolująca wszystkie pobierane przez przeglądarkę dane.
17. Zapora sieciowa.
18. Kontrola dostępu do urządzeń USB.
19. Moduł skanowania rejestru systemowego.
20. Zaawansowane mechanizmy ochronne oparte o chmurę producenta.
21. W pełni automatyczny mechanizm aktualizacji zarówno baz wirusów jak i modułów programu nie wymagający ingerencji użytkownika.
22. Zaawansowany mechanizm raportowania obejmujący wszystkie istotne z punktu widzenia funkcjonowania pakietu zdarzenia.
23. Możliwość zabezpieczenia hasłem konfiguracji pakietu.
24. Pomoc techniczna dla programu świadczona w języku polskim.

25. Możliwość zdalnego połączenia (za zgodą użytkownika) z komputerem klienta przez wykwalifikowanego pracownika wsparcia technicznego producenta w celu rozwiązania problemów wskazanych przez użytkownika.
26. Moduł Administracyjny do zdalnego zarządzania instalacjami pakietu w sieci z konsolą dostępną z poziomu przeglądarki.

Skaner na żądanie

1. Możliwość skanowania wszystkich zasobów komputera.
2. Mechanizm szybkiego skanowania pozwalający na sprawdzenie najważniejszych zasobów komputera. Skanowanie szybkie może być uruchomione:
   - Na żądanie.
   - Po starcie systemu.
   - Po zalogowaniu użytkownika.
   - Po aktualizacji baz wirusów.
3. Możliwość tworzenia wielu profili skanowania obejmujących wybrane przez użytkownika zasoby oraz indywidualne ustawienia.
4. Możliwość definiowania harmonogramów skanowania dla poszczególnych profili
5. Możliwość uruchomienia skanowania wybranych zasobów z poziomu menu kontekstowego (prawoklik)
6. Możliwość skanowania wskazanych zasobów z linii poleceń (tzw. skaner command-line)
7. Możliwość skanowania zasobów komputera w trybie awaryjnym Windows

Monitor antywirusowy/ochrona plików

1. Analiza wszystkich uruchamianych/otwieranych/kopiowanych/pobieranych plików.
2. Mechanizm uniemożliwiający dostęp do zainfekowanych obiektów.
3. Możliwość definiowania akcji podejmowanych przez monitor w przypadku wykrycia szkodliwego pliku:
   - Leczenie pliku (lub jego usunięcie w przypadku, gdy lecznie nie jest możliwe).
   - Kasowanie pliku.
   - Przeniesienie pliku do kwarantanny.
   - Pytanie do użytkownika - w tym wypadku program wyświetla okno z pytaniem o akcję, która ma zostać podjęta.
4. Możliwość natychmiastowego wysłania zainfekowanego pliku do producenta w celu jego dalszej analizy.
5. Możliwość włączenia/wyłączenia skanowania plików na zasobach sieciowych.
6. Możliwość zablokowania mechanizmów autostartu na nośnikach zewnętrznych (np. autorun.inf na nośnikach USB).
7. Możliwość definiowania listy plików i folderów wyłączonych z ochrony antywirusowej.
8. Możliwość czasowej deaktywacji monitora antywirusowego na 10 minut albo do ponownego uruchomienia systemu.

Kontrola rodzicielska/Kontrola dostępu

1. Baza danych szkodliwych treści podzielona na kategorie pozwalająca na dostosowanie poziomu ochrony do wieku i wymagań użytkowników.
2. Możliwość definiowania indywidualnych ustawień ochrony dla każdego użytkownika systemu.
3. Możliwość definiowania reguł obejmujących strony dopuszczane i blokowane zarówno na podstawie adresów stron jak i na podstawie ich treści.
4. Możliwość włączenia trybu bezpiecznego wyszukiwania.
5. Możliwość zablokowania pobierania programów z Internetu.
6. Możliwość definiowania tygodniowego harmonogramu dostępu do Sieci.
7. Dostęp do historii przeglądanych stron indywidualnie dla każdego użytkownika systemu z możliwością natychmiastowego dodawania adresów z listy do bazy stron blokowanych lub dopuszczanych.

Ochrona poczty

1. Skanowanie poczty przesyłanej protokołami POP3/SMTP/IMAP.
2. Skanowanie połączeń szyfrowanych SSL.
3. Skanowanie nie wymaga zmiany ustawień kont pocztowych (adres serwera/użytkownik itp.) i działa niezależnie od używanego klienta pocztowego.
4. Mechanizm wykrywający i zabezpieczający przed uruchomieniem/otworzeniem potencjalnie szkodliwych załączników w formacie popularnych dokumentów/skryptów/programów wykonywalnych.
5. Możliwość usunięcia zainfekowanych listów lub obudowania ich w strukturze bezpiecznego załącznika.
6. Moduł antyspamowy oparty o sztuczną inteligencję zaimplementowaną przez producenta z możliwością definiowania własnych reguł przez użytkownika opartą między innymi o historię korespondencji.

Ochrona przeglądarki

1. Skanowanie całego ruchu realizowanego za pośrednictwem przeglądarek internetowych niezależnie od ich wersji.
2. Skanowanie połączeń szyfrowanych.
3. Możliwość definiowania listy domen wykluczonych ze skanowania.
4. Zaawansowany mechanizm skanowania i analizy załączników pocztowych w ramach wszystkich popularnych serwisów pocztowych - gmail, onet, wp, tlen, microsoft itp.

Bezpieczna przeglądarka internetowa

1. Kontrola uruchomionych aplikacji.
2. Ochrona przed 'wstrzykiwaniem' bibliotek do przeglądarki.

3. Filtr antyphishingowy.
4. Kontrola przekierowania ruchu sieciowego.
5. Ochrona schowka systemowego.
6. Ochrona pliku hosts.

Zapora sieciowa

1. Kontrola całego ruchu sieciowego w kontekście adresów oraz aplikacji.
2. Możliwość tworzenia reguł zapory zarówno dla adresów/portów jak i aplikacji oraz folderów lokalnych.
3. Tryb pracy interaktywnej oraz cichej, opartej na już stworzonych regułach.
4. W trybie interaktywnym, dla nowych połączeni program podaje szczegółowe informacje dotyczące zarówno adresów i portów jak i aplikacji realizującej połączenie. Użytkownik może podjąć decyzję o blokowaniu/przepuszczeniu połączenia oraz utworzenia reguły dla połączeń późniejszych.
5. Możliwość wyłączenia kontroli zapory dla połączeń realizowanych w ramach sieci lokalnych.
6. Możliwość definiowania sieci lokalnych.
7. Możliwość wyłączenia kontroli zapory dla połączeń wychodzących.
8. Funkcja blokowania aktywności sieciowej skryptów.

Kontrola dostępu do urządzeń USB

1. Możliwość zdefiniowania reguł dostępu do urządzeń USB indywidualnie dla każdego użytkownika systemu:
   - Możliwość zablokowania dostępu do nośników USB.
   - Możliwość zablokowania zapisu na nośnikach USB.
   - Możliwość zablokowania dostępu do drukarek.
   - Możliwość zablokowania dostępu do kart sieciowych USB.
2. Mechanizm automatycznego skanowania nośników USB podłączanych do komputera.

Ochrona w chmurze

1. Możliwość włączenia przez użytkownika mechanizmów wspierających ochronę systemu danymi pochodzącymi z chmury producenta.
   - Anonimowa reputacji pracujących w systemie aplikacji.
   - Weryfikacja potencjalnych zagrożeń (skryptów, makr itp.) w chmurze producenta.

Aktualizacja pakietu

1. Tryb automatycznej aktualizacji pobierający najnowsze bazy wirusów i moduły programu z serwerów producenta lub z repozytorium tworzonego u użytkownika.
2. Możliwość tworzenia indywidualnego harmonogramu aktualizacji.
3. Możliwość tworzenia repozytorium aktualizacji i udostępniania go w sieci innym komputerom z wykorzystaniem protokołu http lub zasobu lokalnego.
4. Możliwość odroczenia aktualizacji plików wykonywalnych i bibliotek pakietu.
5. Współpraca z serwerami proxy.

Raporty

1. Program tworzy raporty obejmujące wszystkie istotne z punktu widzenia jego funkcjonowania zdarzenia:
   - Wykryte infekcje oraz wykonane akcje.
   - Zainfekowana poczta.
   - Infekcje na stronach WWW.
   - Nowe połączenia analizowane przez zaporę sieciową.
   - Zablokowane strony w ramach kontroli rodzicielskiej (raporty przyrostowe).
   - Aktualizacja pakietu.
   - Utworzenie kopii zapasowej.
2. Mechanizm kasowania raportów starszych niż 30 dni.
3. Przeglądarka raportów oferująca dostęp do zdarzeń z wybranego dnia.

Narzędzia dodatkowe i bezpieczeństwo danych

1. Mechanizm aktywnej ochrony dokumentów użytkownika SafeStorage pozwalający na odzyskanie utraconych danych np. w efekcie działania zagrożeń typu Tesla Crypt czy Crypto Locker.
Technologia SafeStorage pozwala również na ochronę plików znajdujących się na zasobach sieciowych.
2. Własny menadżer procesów dający dostęp do najważniejszych informacji o uruchomionych w systemie aplikacjach oraz o ich reputacji w oparciu o dane pochodzące z chmury producenta.
3. Moduł kwarantanny pozwalający na bezpieczne przechowywanie zainfekowanych lub podejrzanych plików.
4. Moduł pozwalający na tworzenie kopii zapasowych ważnych dla użytkownika plików, oferujący między innymi:
   - Możliwość tworzenia wielu profili kopii zapasowych obejmujących wybrane przez użytkownika zasoby.
   - Możliwość tworzenia pełnych kopii zapasowych lub kopii przyrostowych.
   - Możliwość wygodnego definiowania harmonogramu tworzenia kopii zapasowych.
   - Możliwość wygodnego odzyskiwania zarchiwizowanych danych z wybranej wersji kopii zapasowej.
   - Możliwość tworzenia kopii zapasowych na dyskach sieciowych.

5. Mechanizm pozwalający na wygenerowania szczegółowego raportu o systemie z możliwością wysłania go do producenta w celu analizy potencjalnych problemów w systemie użytkownika.
6. Mechanizm generacji płyty ratunkowej lub pendrive'a ratunkowego pozwalających na awaryjne uruchomienie komputera w przypadku awarii systemu.

Ochrona urządzeń mobilnych z systemem Android
1. Prosta instalacja za pomocą instalatora APK.
2. Skanowanie istotnych zasobów systemu pod kątem infekcji.
3. Wykrywanie aplikacji o potencjalnie zbyt wysokich uprawnieniach.
4. Automatyczne skanowanie systemu po instalacji nowych aplikacji.
5. Możliwość blokowania określonych aplikacji za pomocą hasła administracyjnego pakietu Arcabit.
6. Automatyczna aktualizacja baz zagrożeń.
7. Możliwość wykorzystania zasobów chmury do skanowania systemu.

Moduł administracyjny do zarządzania instalacjami pakietu w sieci
1. Serwer zarządzający nie wymagających zewnętrznych mechanizmów bazodanowych.
2. Konsola administracyjna dostępna z poziomu przeglądarki internetowej pozwalająca na zdalny dostęp do serwera zarządzającego.
3. Możliwość tworzenia rozbudowanej struktury grup i podgrup zarządzanych stacji.
4. Automatyczne tworzenie repozytorium aktualizacyjnego dla zarządzanych stacji.
5. Możliwość definiowania indywidualnych ustawień dla każdej grupy i maszyny.
6. Blokada możliwości zmiany ustawień i aktywności modułów ochronnych przez użytkowników na stacjach roboczych.
7. Zaawansowany system zbierania i przeglądania raportów i informacji o zdarzeniach w sieci.
8. Kontrola aplikacji uruchamianych na zarządzanych stacjach roboczych pozwalająca na:
   - Włączenie/wyłączenie możliwości uruchamiania wszystkich aplikacji z folderu Program Files
   - Włączenie/wyłączenie możliwości uruchamiania wszystkich aplikacji przez użytkowników o uprawnieniach administracyjnych.
   - Definiowanie listy aplikacji dopuszczonych lub zablokowanych na podstawie ścieżki lub sumy kontrolnej pliku.
9. Możliwość zdalnego uruchomienia skanowania i aktualizacji na stacjach.
10. Dostęp do listy uruchomionych procesów na zarządzanych stacjach.
11. Informacja o zasobach sprzętowych zarządzanych stacji (procesor/pamięć/napędy/wersja systemu operacyjnego).
12. Możliwość zdalnego uruchomienia procesu/skryptu na zarządzanych stacjach z wykorzystaniem uprawnień użytkownika zalogowanego na stacji lub z wykorzystaniem uprawnień administracyjnych.
13. Możliwość zdalnego podglądu pulpitu zarządzanych stacji.
14. Kontrola liczby stanowisk w kontekście wykorzystywanej przez użytkownika licencji.
15. Możliwość zdalnego wyłączenia/ponownego uruchomienia/zablokowanie wybranych stacji.
16. Możliwość zdalnego uruchomienia wybranych stacji (funkcja Wake-on-LAN).
17. Współpraca z serwerami proxy.
18. Możliwość prostego przeniesienia stacji do innego serwera zarządzającego bezpośrednio z poziomu konfiguracji w konsoli.
19. Możliwość wysyłania mailowych powiadomień o wykrytych w sieci zagrożeniach.
20. Narzędzie do skanowania sieci w poszukiwaniu stacji niezarządzanych przez moduł administracyjny.

16. w zał. nr 5 do SIWZ – Opis przedmiotu zamówienia, sekcja „5.11 Zakup sprzętu i oprogramowania komputerowego", opis dla **„Urządzenia wielofunkcyjne mono – 15 szt."** wiersz 12 otrzymuje brzmienie:

Przed modyfikacją:

12.	Czcionki drukarki	89 PCL Latin 91 PostScript 3 Emulation Latin

Po modyfikacji:

12.	Czcionki drukarki	~~89~~ 84 PCL Latin 91 PostScript 3 Emulation Latin

17. w zał. nr 5 do SIWZ – Opis przedmiotu zamówienia, sekcja „5.12 Zapewnienie bezpieczeństwa przesyłanych informacji", opis dla **„Urządzenie ochrony sieci – 1szt. pracujące w klastrze HA z użytkowanym"** po tabeli z opisem wymagań minimalnych dodaje się zapisy:

LUB ROZWIĄZANIE Urządzenie ochrony sieci – 1szt. pracujące w klastrze HA z użytkowanym:

Element konfiguracji	Wymagania minimalne
Licencjonowanie	Oferowane rozwiązanie musi być rozwiązaniem programowym umożliwiającym instalację na sprzęcie fizycznym lub jako maszyna wirtualna uruchamiana na wirtualizatorze KVM lub działająca na oferowanej Platformie Wirtualizacyjnej.
	Oprogramowanie musi być dostępne na licencje GPL lub równoważnej, która będzie pozwalała na audyt kodu źródłowego oferowanego rozwiązania.
Funkcjonalności	Zaoferowane oprogramowanie musi posiadać następujące wbudowane funkcjonalności:

	filtrowanie ruchu na podstawie adresów IP źródłowych i docelowych, typu protokołu, portu źródłowego i docelowego TCP i UDP,
	Ustalenia limitów jednoczesnych połączeń z danego hosta źródłowego,
	Możliwość logowania ruchu sieciowego dla wybranych reguł firewalla,
	Tworzenie aliasów do grupowania i nazywania adresów IP, sieci i portów,
	Normalizacje pakietów sieciowych,
	Tworzenie mostów sieciowych warstwy drugiej,
	Tworzenie kolejek sieciowych z podziałem pasma sieciowego,
	Forward pakietów z możliwością stosowania zakresów,
	Translację NAT typu 1:1,
	Translację wyjściową adresów IP na adresy publiczne z możliwością ograniczania portów i protokołów ruchu wychodzącego
	Oferowane oprogramowanie musi działać w oparciu o filtrowanie z uwzględnieniem tablic stanów z następującymi właściwościami: – Ograniczenia w oparciu o ilość jednoczesnych połączeń od klienta – Ograniczenia ilości stanów połączeń z uwzględnieniem danego hosta – Ograniczenia ilości nowych połączeń z uwzględnieniem czasu (per second) – Zarządzanie stanami połączeń: utrzymywania stanu połączeń, brak śledzenia stanu połączeń itp.
	Oferowane oprogramowanie musi oferować funkcjonalność wbudowanego serwera usługi DNS oraz serwera usługi DHCP3,
	Oferowane oprogramowanie musi posiadać wbudowany serwer usługi NTP4,
	Mechanizm wykrywania ataków sieciowych na wskazanych interfejsach sieciowych,
	Wbudowany mechanizmproxy z filtracją ruchu http,
	Wbudowany mechanizm antyspamowy dla ruchu smtp w oparciu o szare listy,
	Zaoferowane oprogramowanie musi posiadać możliwość tworzenia rozwiązań wysokiej dostępności zawierającej minimum dwa węzły. Funkcjonalność wysokiej dostępności musi być dostarczona ze wszystkimi opcjami bez konieczności dokupowania dodatkowych licencji. Jeśli część funkcjonalności wymaga dodatkowych opcji licencyjnych muszą one być dostarczone w momencie oferowania produktu,
	Wbudowany mechanizm VPN musi umożliwiać tworzenie wirtualnych sieci w oparciu o następujące rodzaje VPN: IPsec, OpenVPN i PPTP,
	VPN musi umożliwiać swobodny wybór adresacji sieci IP używanych w tunelach VPN,
	Mechanizm monitorowania ruchu sieciowego i zbierania statystyk z uwzględnieniem typu ruchu, adresów źródłowych i docelowych i graficznej reprezentacji wyników,
Wsparcie	Dla oferowanego systemu do zabezpieczania styku sieci musi być dostarczone wsparcie techniczne, dostępne w języku polskim, oferowane w trybie 24h dostępne za pomocą jednej z wymienionych metod: poczta elektroniczne lub telefon, z nieograniczoną ilością zgłoszeń. **Licencja na 5 lat.**

Zmodyfikowany Zał. nr 5 do SIWZ – „Opis Przedmiotu Zamówienia." zamieszczono na stronie internetowej pod adresem: http://bip.starostwo.ketrzyn.pl/ - zakładka Zamówienia publiczne

Wykonawcy zobowiązani są uwzględnić zmiany wprowadzone modyfikacją SIWZ podczas sporządzania ofert.

Pozostałe zapisy Specyfikacji Istotnych Warunków Zamówienia pozostają bez zmian.

Przygotowała: Marta Szymkiewicz
na podstawie wyjaśnień i dokumentów dostarczonych
przez Panów: Piotra Krakowiaka i Piotra Nowaka

Z up. dyr.

GŁÓWNY KSIĘGOWY
Centrum Usług Wspólnych
Powiatu Kętrzyńskiego
Jolanta Dobrzyńska