**SPECYFIKACJA TECHNICZNA**

**1. System Kopii Bezpieczeństwa**

Zadaniem wykonawcy jest dostarczenie, instalacja i konfiguracja system kopii bezpieczeństwa / archiwizacji wraz z niezbędnym sprzętem.

|  |  |  |  |
| --- | --- | --- | --- |
|  | **Parametry minimalne** | **Parametr wymagany** | **Zgodność z parametrami minimalnymi Tak/Nie** |
| 1.1 | Licencja bez ograniczeń liczby podłączanych urządzeń, oraz przestrzeni dyskowej | Tak |  |
| 1.2 | System umożliwia przesyłanie, archiwizację i udostępnianie obrazów medycznych w standardzie DICOM 3.0 bezpośrednio przez aparaty diagnostyczne | Tak |  |
| 1.3 | Funkcja zdalnego konfigurowania i zarządzania systemem poprzez sieć Internet szyfrowanym protokołem komunikacyjnym | Tak |  |
| 1.4 | Obsługa zewnętrznych macierzy typu NAS bez limitu pojemności i bez konieczności zakupu dodatkowych licencji | Tak |  |
| 1.5 | Automatyczne tworzenie kopii zapasowych obrazów na nośnikach CD/DVD na wewnętrznej nagrywarce CD/DVD i napędach LTO | Tak |  |
| 1.6 | Automatyczne tworzenie kopii zapasowych systemu (baza danych oraz pliki systemu) na nośnikach CD/DVD na wewnętrznej nagrywarce CD/DVD | Tak |  |
| 1.12 | System musi umożliwiać archiwizację i backup danych przesyłanych do archiwum w oparciu o standard DICOM 3.0, min. klasy SOP:  Computed Radiography Image Storage,  Digital X-Ray Image Storage – For Presentation i Processing,  Standard Mammography Image Store – For presentation i Processing,  Standard i Enhanced CT Image Storage,  Ultrasound Standard Image Storage,  Ultrasound Multi-frame Image Storage,  Standard i Enhanced MR Image Storage,  Digital Intra-oral X-Ray Image Storage – For Presentation i Processing,  X-Ray Angiographic Image Storage,  X-Ray Radiofluoroscopic Image Storage,  Nuclear Medicine Image Storage,  Secondary Capture Image Storage,  Multi-Frame Single Bit Secondary Capture Image Storage,  Multi-Frame Grayscale Byte Secondary Capture Image Storage,  Multi-Frame Grayscale Word Secondary Capture Image Storage,  Multi-Frame true Color Secondary Capture Image Storage,  Standalone Overlay Storage,  Standard Modality LUT Storage,  Standard VOI LUT Storage,  Raw Data Storage,  Standard VL Endoscopic Image Storage,  Standard Video Endoscopic Image Storage,  Basic Text SR,  Enhanced SR,  Comprehensive SR,  Mammography CAD SR. | Tak |  |
| 1.14 | Funkcja pozwalająca użytkownikowi na rejestrowanie nowych urządzeń medycznych do bezpośredniego wysyłania badań do archiwizacji i kopii na podstawie parametrów: AET, IP, Port bez potrzeby wzywania serwisu producenta | Tak |  |
| 1.16 | Dokumentacja systemu i instrukcja użytkownika w j.polskim | Tak |  |
| 2.17 | System umożliwia nagrywanie badań pacjentów na nośnikach CD/DVD na wewnętrznej nagrywarce CD/DVD na stacji | Tak |  |
| 2.18 | System umożliwia podłączenie zewnętrznych duplikatorów nagrywających na CD/DVD w celu automatycznego nagrywania płyt z kopiami bezpieczeństwa | Tak |  |
| 2.19 | System umożliwia odtworzenie kopii wybranego badania np. po numerze pesel | Tak |  |

Wraz z system kopii bezpieczeństwa wykonawca musi dostarczyć sprzęt w postaci serwera kopii bezpieczeństwa oraz biblioteki taśmowej, na której będą odkładane kopie oraz zarchiwizowane dane.  
  
**Biblioteka taśmowa z serwerem zarządzającym**

|  |  |  |  |
| --- | --- | --- | --- |
| **1. Serwer Kopi** | | | |
| **Lp.** | Wymagane minimalne parametry techniczne | Wymóg do spełnienia (warunek graniczny) | OFEROWANE PARAMETRY TECHNICZNE – podaje Wykonawca  Wymogi dotyczące opisu oferowanych parametrów:  TAK – rowiązanie spełnia konkretny parametr przy czym Zamawiający oczekuje by w przypadku wymagań dotyczących minimalnych parametrów opisać szczegółowo parametry oferowane przez Wykonawcę  NIE – rozwiązanie nie spełnia konkretnego parametru |
|  | Obudowa  Urządzenie musi być  dostarczone ze wszystkimi  komponentami do instalacji w szafie rack 19 cali | TAK |  |
|  | Napęd LTO-8 | TAK |  |
|  | Sloty na kasety min. 8 | TAK |  |
|  | Interfejs SAS | TAK |  |
|  | prędkość przesyłu min: 270MB/s | TAK |  |
|  | Obsługa taśm WORM | TAK |  |
|  | Dołączone 10 szt. 30TB RW oraz 1 szt.  nośniki taśm czyszczących | TAK |  |
|  | **Serwer** | | |
|  | obudowa do montażu w szafie typu rack | TAK |  |
|  | zasilanie redundantne, przynajmniej 2 zasilacze typu HotPlug | TAK |  |
|  | płyta główna z możliwością zainstalowania minimum dwóch procesorów | TAK |  |
|  | zegar procesora minimum 3,0 GHz | TAK |  |
|  | zainstalowane 1 procesory minimum ośmiordzeniowy klasy x86 dedykowane do pracy w serwerach, zaprojektowane do pracy w układach wieloprocesorowych | TAK |  |
|  | pamięć minimum 128GB ECC DIMM, rozszerzalna, z zabezpieczeniem typu: ECC | TAK |  |
|  | Kontroler Raid z minimum 2GB pamięci cache  dyski minimum 2x 960 GB SSD skonfigurowane w RAID1 , 2x16TB 7,2k HDD | TAK |  |
|  | sieć minimum, 2x10Gb SFP+ SR, 2x1Gb RJ45 | TAK |  |
|  | Zarządzanie:   * Zintegrowany z płytą główną serwera, niezależny od systemu operacyjnego, sprzętowy kontroler zdalnego zarządzania * Monitoring statusu i zdrowia systemu * Logowanie zdarzeń * Umożliwiający Update systemowego firmware * Umożliwiającyzdalnąkonfiguracjęserwera * Monitoring i możliwość ograniczenia poboru prądu * Zdalnewłączanie/wyłączanie/restart * Przekierowanie konsoli szeregowej przez IPMI * Zrzut ekranu w momencie zawieszenia system * Możliwość przejęcia zdalnego ekranu 1920x1200, 60 Hz,16 bpp * Zdalnydostęp do serwera * Możliwość zdalnej instalacji systemu operacyjnego * Alerty Syslog * Przekierowanie konsoli szeregowej przez SSH * Wyświetlanie danych aktualnych I historycznych dla użycia energii I temperatury serwera * Możliwość mapowania obrazów ISO z lokalnego dysku operatora * Możliwość mapowania obrazów ISO przez HTTPS * Możliwość jednoczesnej pracy użytkowników przez wirtualną konsolę * Wspierane protokoły/interfejsy: IPMI v2.0, SNMP v3 | TAK |  |
|  | gwarancja: min. 24 m-cy, 3YNBD, producenta | TAK |  |

**2. System ochrony poczty email**

Przedmiotem zamówienia jest dostawa oprogramowania klasy korporacyjnej, które zapewnia o ochronę poczty wychodzącej i przychodzącej firm przed phishingiem, oprogramowaniem ransomware, spamem, wirusami i inne zaawansowane zagrożenia e-mail, zanim dotrą do sieci. Zapewnia zaawansowaną ochronę dla MicrosoftTM Exchange Server, MicrosoftTM Office 365, GoogleTM G Suite i inne hostowane lub lokalne rozwiązania e-mailowe. Ochroną ma zostać objętych min. 60 skrzynek pocztowych w jednej domenie przez okres min. 24 miesięcy

Wymagania ogólne

Rozwiązanie musi być dostarczone w formie SaaS, gdzie centralny serwer hostowany jest w chmurze i dostarczony przez producenta oferowanego rozwiązania jako usługa. Producent oferowanego rozwiązania jest odpowiedzialny za niezawodność, skalowalność oraz aktualizacje wszystkich elementów centralnych dostarczanych jako usługa typu SaaS.

Rozwiązanie ma udostępniać konsolę:

* Z opcją pojedynczego uwierzytelniania SSO, Single Sign-On - za pomocą SAML: wsparcie dla Azure AD, AD FS oraz Okta
* wykorzystujący Interfejs zarządzający, który musi być obsługiwany przez poniższe przeglądarki internetowe:
  + Internet Explorer 11 lub nowszy
  + Mozilla Firefox 34 lub nowszy
  + Google Chrome 35 lub nowsze
* Z dostępem przez interfejs programistyczny API zapewniający tworenie zapytań, dodawania, usuwania na zasobach

W celu aktywowania rozwiazania niezbędne jest:

* Posiadanie Email Gateway’a
* Dostęp do danych zapisanych w rekorda MX

Wymagania funkcjonalne rozwiązania:

* musi działać poprzez przechwytywanie wiadomości e-mail klientów za pośrednictwem przekierowywanie rekordów MX serwerów poczty przychodzącej do oferowanego systemu.
* musi mieć wbudowane mechanizmy ochrony na poziomie akceptacji bądź odrzucenia przychodzących połączeń SMTP, z wykorzystaniem przynajmniej następujących mechanizmów:
  + Lista reputacyjna dostarczana przez producenta rozwiązania
  + Czarne i białe listy definiowane przez administratora
  + SPF – Sender Policy Framework
  + DKIM – DomainKeysIdentified Mail - uwierzytelnienie i podpisy dla ruchu wychodzącego
  + DMARC - Domain-based Message Authentication, Reporting and Conformance
* Musi zapewniać ochronę poczty wychodzącej wykorzystując mechanizmy:
  + Reputacji IP odbiorcy
  + Weryfikacji TLS
  + Ochrony antywirusowej
  + Ochrony antyspamowej
  + Analizy treści
  + DLP
  + Innych polityk tworzynych przez administratorów rozwiązania
* musi zapewnić ochronę przed spamem, phishingiem i graymail za pomocą wielu technik, w tym reputacji nadawcy, analizy treści i obrazu, machine learning i innych.
* musi zapewnić ochronę przed złośliwymi skryptami w plikach PDF, MicrosoftTM Office i innych dokumentach przy użyciu logiki statycznej i heurystycznej w celu wykrywania i badania nieprawidłowości.
* musi zapewnić ochronę przez zagrożeniami Zero-day przez wykorzystanie analizy machine learning na etapie przed uruchomieniem.
* musi wykorzystywać bazę reputayjną adresów URL w celu blokowania złośliwych adresów URL osadzonych w wiadomościach e-mail.
* musi umożliwiać ochronę czasu kliknięcia (Time-of-Click), która blokuje wiadomości e-mail ze złośliwymi adresami URL przed dostarczeniem i ponownie sprawdza bezpieczeństwo adresów URL, gdy użytkownik końcowy kliknie na podejrzany URL.
* musi posiadać mechanizm ochrony przed wyciekiem danych (DLP) dla OneDrive, Teams oraz Sharepoint, umożliwiający co najmniej:
  + Blokowanie na podstawie predefiniowanych wzorców
  + Definiowanie własnych identyfikatorów danych z użyciem wyrażeń regularnych (regex)
  + Tworzenie reguł, z wykorzystaniem własnych oraz wbudowanych list słów kluczowych i identyfikatorów danych
  + Wykorzystania reguł DLP do monitorowania także ruchu poczty elektronicznej
  + Posiadający wbudowane polskie identyfikatory ochrony danych, przynajmniej dla:
    - Pesel
    - Numer Dowodu Osobistego
    - Numer rachunku bankowego
    - Numer telefonu
    - Blokowanie na podstawie listy statycznej słów kluczowych
* musi zapewnić filtrowanie treści pod kątem zdefiniowanych wyrażeń występujących w nagłówkach, temacie i treści maila przychodzącego lub wychodzącego:
  + Możliwość zdefiniowania wyrażeń regularnych posixprzez administratora
  + Możliwość użycia zdefiniowanych lub zdefiniowania przez administratora słów kluczowych
* musi posiadać wskazane limity dotyczące obsługi poczty elektronicznej
  + Maksymalna wielkość email – 50 MB
  + Maksymalny czas dostępu do danych połączenia wykonanego przy dostarczeniu mail’a – 30 dni
  + Maksymalny czas dostępu do mail umieszczonego w kwarantannie – 30 dni
* musi posiadać funkcjonalność eksportu do pliku csv danych dotyczących naruszeń utworzonych przez administratora polityk, które zawierają następujące informacje:
  + czas
  + nadawca
  + odbiorca
  + nazwa zagrożenia
  + typ
  + nazwa mechanizmu
  + podjęta akcja
  + temat
  + ID wiadomości
  + wielkość wiadomości
  + wychodząca/przychodząca
  + nazwa polityki
* musi pozwalać na przekazanie zdarzeń do systemów zewnętrznych przy pomocy syslog w formacie CEF/LEEF
* musi posiadać konsolę użytkownika końcowego jako niezależny portal, w którym użytkownicy końcowi mogą się logować i zarządzać swoimi wiadomościami typu: spam i graymail, wiadomości e-mail poddane kwarantannie, mogę skonfigurować własne white/black listy nadawców.
* musi umożliwiać zdefiniowanie powiadomień o wykrytych zagrożeniach odrębnie dla użytkowników i administratorów systemu
* musi posiadać wbudowany mechanizm generowania raportów, tworzenia dashboard’ów

W celu potwierdzenia zgodności oferowanych rozwiązań z wymaganiami określonymi w opisie systemu ochrony poczty e-mail przedmiotu zamówienia Zamawiający żąda złożenia wraz z ofertą:

Opisu technicznego oferowanego rozwiązania, folderów, kart katalogowych lub instrukcji obsługi wraz ze wskazaniem wszystkich parametrów technicznych, w zakresie umożliwiającym ocenę spełniania wymagań zamawiającego określonych w SWZ i Specyfikacji technicznej oraz oświadczenia wytwórcy lub autoryzowanego dystrybutora o spełnianiu wymaganych parametrów. W przypadku załączenia oświadczenia autoryzowanego dystrybutora należy przedłożyć stosowne upoważnienie do reprezentowania wytwórcy.