

## Opis Przedmiotu zamówienia

### I. ZAAWANSOWANY SYSTEM ANTYWIRUSOWY

Niniejsza specyfikacja określa wymagania dotyczące zakupu i wdrożenia rozwiązania bezpieczeństwa dla Zleceniodawcy. Celem jest zapewnienie kompleksowej ochrony przed zagrożeniami zewnętrznymi, wirusami, malware, oraz wzmocnienie bezpieczeństwa danych i zasobów.

**Ilość wymaganych licencji: 27 na okres 24 miesięcy**

**Minimalny zakres jaki musi spełniać dostarczony sprzęt/oprogramowanie:**

#### **Administracja zdalna w chmurze:**

1. Rozwiązanie musi być dostępne w chmurze producenta oprogramowania antywirusowego.
2. Rozwiązanie musi umożliwiać dostęp do konsoli centralnego zarządzania z poziomu interfejsu WWW.
3. Rozwiązanie musi być zabezpieczone za pośrednictwem protokołu SSL.
4. Rozwiązanie musi posiadać mechanizm wykrywający sklonowane maszyny na podstawie unikatowego identyfikatora sprzętowego stacji.
5. Rozwiązanie musi posiadać możliwość komunikacji agenta przy wykorzystaniu http Proxy.
6. Rozwiązanie musi posiadać możliwość zarządzania urządzeniami mobilnymi – MDM.
7. Rozwiązanie musi posiadać możliwość wymuszenia dwufazowej autoryzacji podczas logowania do konsoli administracyjnej.
8. Rozwiązanie musi posiadać możliwość dodania zestawu uprawnień dla użytkowników w oparciu co najmniej o funkcje zarządzania: politykami, raportowaniem, zarządzaniem licencjami, zadaniami administracyjnymi. Każda z funkcji musi posiadać możliwość wyboru uprawnienia: odczyt, użyj, zapisz oraz brak.
9. Rozwiązanie musi posiadać minimum 80 szablonów raportów, przygotowanych przez producenta.
10. Rozwiązanie musi posiadać możliwość tworzenia grup statycznych i dynamicznych komputerów.
11. Grupy dynamiczne muszą być tworzone na podstawie szablonu określającego warunki, jakie musi spełnić klient, aby został umieszczony w danej grupie. Warunkiem są zawierać co najmniej: adresy sieciowe IP, aktywne zagrożenia, stan funkcjonowania/ochrony, wersja systemu operacyjnego, podzespoły komputera.
12. Rozwiązanie musi posiadać możliwość uruchomienia zadań automatycznie, przynajmniej z wyzwalaczem: wyrażenie CRON, codziennie, cotygodniowo, comiesięcznie, corocznie, po wystąpieniu nowego zdarzenia oraz umieszczeniu agenta w grupie dynamicznej.

#### **Ochrona stacji roboczych:**

13. Rozwiązanie musi wspierać systemy operacyjne Windows (Windows 10/Windows 11).

**Dostawa sprzętu sieciowego i oprogramowania na potrzeby Gminy Cielądz  
w ramach programu “Cyberbezpieczny Samorząd”**

Or.SO.2714.13.2024

14. Rozwiązanie musi wspierać architekturę ARM64.
15. Rozwiązanie musi zapewniać wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor.
16. Rozwiązanie musi posiadać wbudowaną technologię do ochrony przed rootkitami oraz podłączeniem komputera do sieci botnet.
17. Rozwiązanie musi zapewniać wykrywanie potencjalnie niepożądanych, niebezpiecznych oraz podejrzanych aplikacji.
18. Rozwiązanie musi zapewniać skanowanie całego dysku, wybranych katalogów lub pojedynczych plików "na żądanie" lub według harmonogramu.
19. Rozwiązanie musi zapewniać skanowanie plików spakowanych i skompresowanych oraz dysków sieciowych i dysków przenośnych.
20. Rozwiązanie musi posiadać opcję umieszczenia na liście wykluczeń ze skanowania wybranych plików, katalogów lub plików na podstawie rozszerzenia, nazwy, sumy kontrolnej (SHA1) oraz lokalizacji pliku.
21. Rozwiązanie musi integrować się z Intel Threat Detection Technology.
22. Rozwiązanie musi zapewniać skanowanie i oczyszczanie poczty przychodzącej POP3 i IMAP „w locie” (w czasie rzeczywistym), zanim zostanie dostarczona do klienta pocztowego, zainstalowanego na stacji roboczej (niezależnie od konkretnego klienta pocztowego).
23. Rozwiązanie musi zapewniać skanowanie ruchu sieciowego wewnątrz szyfrowanych protokołów HTTPS, POP3S, IMAPS.
24. Rozwiązanie musi posiadać wbudowane dwa niezależne moduły heurystyczne – jeden wykorzystujący pasywne metody heurystyczne i drugi wykorzystujący aktywne metody heurystyczne oraz elementy sztucznej inteligencji. Musi istnieć możliwość wyboru, z jaką heurystyka ma odbywać się skanowanie – z użyciem jednej lub obu metod jednocześnie.
25. Rozwiązanie musi zapewniać blokowanie zewnętrznych nośników danych na stacji w tym przynajmniej: Pamięci masowych, optycznych pamięci masowych, pamięci masowych Firewire, urządzeń do tworzenia obrazów, drukarek USB, urządzeń Bluetooth, czytników kart inteligentnych, modemów, portów LPT/COM oraz urządzeń przenośnych.
26. Rozwiązanie musi posiadać funkcję blokowania nośników wymiennych, bądź grup urządzeń ma umożliwiać użytkownikowi tworzenie reguł dla podłączanych urządzeń minimum w oparciu o typ, numer seryjny, dostawcę lub model urządzenia.
27. Moduł HIPS musi posiadać możliwość pracy w jednym z pięciu trybów:
  - tryb automatyczny z regułami, gdzie program automatycznie tworzy i wykorzystuje reguły wraz z możliwością wykorzystania reguł utworzonych przez użytkownika,
  - tryb interaktywny, w którym to rozwiązanie pyta użytkownika o akcję w przypadku wykrycia aktywności w systemie,
  - tryb oparty na regułach, gdzie zastosowanie mają jedynie reguły utworzone przez użytkownika,
  - tryb uczenia się, w którym rozwiązanie uczy się aktywności systemu i użytkownika oraz tworzy odpowiednie reguły w czasie określonym przez użytkownika. Po wygaśnięciu tego czasu program musi samoczynnie przełączyć się w tryb pracy

- oparty na regułach,
- tryb inteligentny, w którym rozwiązanie będzie powiadamiało wyłącznie oszczególnie podejrzanych zdarzeniach.
28. Rozwiązanie musi być wyposażone we wbudowaną funkcję, która wygeneruje pełny raport na temat stacji, na której zostało zainstalowane, w tym przynajmniej z: zainstalowanych aplikacji, usług systemowych, informacji o systemie operacyjnym i sprzęcie, aktywnych procesów i połączeń sieciowych, harmonogramu systemu operacyjnego, pliku hosts, sterowników.
29. Funkcja, generująca taki log, ma posiadać przynajmniej 9 poziomów filtrowania wyników pod kątem tego, które z nich są podejrzane dla rozwiązania i mogą stanowić zagrożenie bezpieczeństwa.
30. Rozwiązanie musi posiadać automatyczną, inkrementacyjną aktualizację silnika detekcji.
31. Rozwiązanie musi posiadać tylko jeden proces uruchamiany w pamięci, z którego korzystają wszystkie funkcje systemu (antywirus, antyspyware, metody heurystyczne).
32. Rozwiązanie musi posiadać funkcjonalność skanera UEFI, który chroni użytkownika poprzez wykrywanie i blokowanie zagrożeń, atakujących jeszcze przed uruchomieniem systemu operacyjnego.
33. Rozwiązanie musi posiadać ochronę antyspamową dla programu pocztowego Microsoft Outlook.
34. Zapora osobista rozwiązania musi pracować w jednym z czterech trybów:
- tryb automatyczny – rozwiązanie blokuje cały ruch przychodzący i zezwala tylko na połączenia wychodzące,
  - tryb interaktywny – rozwiązanie pyta się o każde nowo nawiązywane połączenie,
  - tryb oparty na regułach – rozwiązanie blokuje cały ruch przychodzący i wychodzący, zezwalając tylko na połączenia skonfigurowane przez administratora,
  - tryb uczenia się – rozwiązanie automatycznie tworzy nowe reguły zezwalające na połączenia przychodzące i wychodzące. Administrator musi posiadać możliwość konfigurowania czasu działania trybu.
35. Rozwiązanie musi być wyposażona w moduł bezpiecznej przeglądarki.
36. Przeglądarka musi automatycznie szyfrować wszelkie dane wprowadzane przez Użytkownika.
37. Praca w bezpiecznej przeglądarce musi być wyróżniona poprzez odpowiedni kolor ramki przeglądarki oraz informację na ramce przeglądarki.
38. Rozwiązanie musi być wyposażone w zintegrowany moduł kontroli dostępu do stron internetowych.
39. Rozwiązanie musi posiadać możliwość filtrowania adresów URL w oparciu o co najmniej 140 kategorii i podkategorii.
40. Rozwiązanie musi zapewniać ochronę przed zagrożeniami 0-day.
41. W przypadku stacji roboczych rozwiązanie musi posiadać możliwość wstrzymania uruchamiania pobieranych plików za pośrednictwem przeglądarek internetowych, klientów poczty e-mail, z nośników wymiennych oraz wyodrębnionych z archiwum.

**Ochrona serwera:**

42. Rozwiązanie musi wspierać systemy Microsoft Windows Server 2012 i nowszych oraz Linux w tym co najmniej: RedHat Enterprise Linux (RHEL) 7,8 i 9, CentOS 7, Ubuntu Server 18.04 LTS i nowsze, Debian 10, Debian 11 i Debian 12, SUSE Linux Enterprise Server (SLES) 15, Oracle Linux 8 oraz Amazon Linux.
43. Rozwiązanie musi zapewniać ochronę przed wirusami, trojanami, robakami i innymi zagrożeniami.
44. Rozwiązanie musi zapewniać wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor.
45. Rozwiązanie musi zapewniać możliwość skanowania dysków sieciowych typu NAS.
46. Rozwiązanie musi posiadać wbudowane dwa niezależne moduły heurystyczne – jeden wykorzystujący pasywne metody heurystyczne i drugi wykorzystujący aktywne metody heurystyczne oraz elementy sztucznej inteligencji. Rozwiązanie musi istnieć możliwość wyboru, z jaką heurystyka ma odbywać się skanowanie – z użyciem jednej lub obu metod jednocześnie.
47. Rozwiązanie musi wspierać automatyczną, inkrementacyjną aktualizację silnika detekcji.
48. Rozwiązanie musi posiadać możliwość wykluczania ze skanowania procesów.
49. Rozwiązanie musi posiadać możliwość określenia typu podejrzanych plików, jakie będą przesyłane do producenta, w tym co najmniej pliki wykonywalne, archiwa, skrypty, dokumenty.

**Dodatkowe wymagania dla ochrony serwerów Windows:**

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

**Dodatkowe wymagania dla ochrony serwerów Linux:**

- 59. Rozwiązanie musi pozwalać, na uruchomienie lokalnej konsoli administracyjnej, działającej z poziomu przeglądarki internetowej.
- 60. Lokalna konsola administracyjna nie może wymagać do swojej pracy, uruchomienia instalacji dodatkowego rozwiązania w postaci usługi serwera Web.
- 61. Rozwiązanie, do celów skanowania plików na macierzach NAS / SAN,
- 62. Rozwiązanie musi działać w architekturze bazującej na technologii mikro-serwisów. Funkcjonalność ta musi zapewniać podwyższony poziom stabilności, w przypadku awarii jednego z komponentów rozwiązania, nie spowoduje to przerwania pracy całego procesu, a jedynie wymusi restart zawieszonoego mikro-serwisu.

**Szyfrowanie:**

- 63. System szyfrowania danych musi wspierać instalację aplikacji klienckiej w środowisku Microsoft Windows 7/8/8.1/10 32-bit i 64-bit.
- 64. System szyfrowania musi wspierać zarządzanie natywnym szyfrowaniem w systemach macOS (FileVault).
- 65. Aplikacja musi posiadać autentykację typu Pre-boot, czyli uwierzytelnienie użytkownika zanim zostanie uruchomiony system operacyjny. Musi istnieć także możliwość całkowitego lub czasowego wyłączenia tego uwierzytelnienia.
- 66. Aplikacja musi umożliwiać szyfrowanie danych tylko na komputerach z UEFI.

**Ochrona urządzeń mobilnych opartych o system Android:**

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



- i. uprawnienia aplikacji,
- j. pochodzenie aplikacji z nieznanego źródła.

### **Sandbox w chmurze:**

- 74. Rozwiązanie musi zapewniać ochronę przed zagrożeniami 0-day.
- 75. Rozwiązanie musi wykorzystywać do działania chmurę producenta.
- 76. Rozwiązanie musi posiadać możliwość określenia jakie pliki mają zostać przesłane do chmury automatycznie, w tym archiwa, skrypty, pliki wykonywalne, możliwy spam, dokumenty oraz inne pliki typu .jar, .reg, .msi.
- 77. Administrator musi mieć możliwość zdefiniowania po jakim czasie przesłane pliki muszą zostać usunięte z serwerów producenta.
- 78. Administrator musi mieć możliwość zdefiniowania maksymalnego rozmiaru przesyłanych próbek.
- 79. Rozwiązanie musi pozwalać na utworzenie listy wykluczeń określonych plików lub folderów z przesyłania.
- 80. Po zakończonej analizie pliku, rozwiązanie musi przysyłać wynik analizy do wszystkich wspieranych produktów.
- 81. Administrator musi mieć możliwość podejrzenia listy plików, które zostały przesłane do analizy.
- 82. Rozwiązanie musi pozwalać na analizowanie plików, bez względu na lokalizację stacji roboczej. W przypadku wykrycia zagrożenia, całe środowisko jest bezzwłocznie chronione.
- 83. Rozwiązanie nie może wymagać instalacji dodatkowego agenta na stacjach roboczych.
- 84. Rozwiązanie pozwala na wysłanie dowolnej próbki do analizy przez użytkownika lub administratora, za pomocą wspieranego produktu. Administrator musi móc podejrzec jakie pliki zostały wysłane do analizy oraz przez kogo.
- 85. Przeanalizowane pliki muszą zostać odpowiednio oznaczone. Analiza pliku może zakończyć się z wynikiem:
  - a) Czysty,
  - b) Podejrzany,
  - c) Bardzo podejrzany,
  - d) Szkodliwy.
- 86. W przypadku stacji roboczych rozwiązanie musi posiadać możliwość wstrzymania uruchamiania pobieranych plików za pośrednictwem przeglądarek internetowych, klientów poczty e-mail, z nośników wymiennych oraz wyodrębnionych z archiwum.
- 87. W przypadku serwerów pocztowych rozwiązanie musi posiadać możliwość wstrzymania dostarczania wiadomości do momentu zakończenia analizy próbki.
- 88. Wykryte zagrożenia muszą być przeniesione w bezpieczny obszar kwarantanny, z której administrator może przywrócić dowolne pliki oraz utworzyć dla niej wyłączenia.

### **Moduł XDR:**

- 89. Dostęp do konsoli centralnego zarządzania musi odbywać się z poziomu interfejsu WWW.

90. Serwer administracyjny musi posiadać możliwość wysyłania zdarzeń do konsoli administracyjnej tego samego producenta.
91. Interfejs musi być zabezpieczony za pośrednictwem protokołu SSL.
92. Serwer administracyjny musi posiadać możliwość wprowadzania wykluczeń, po których nie zostanie wyzwolony alarm bezpieczeństwa.
93. Wykluczenia muszą dotyczyć procesu lub procesu „rodzica”.
94. Utworzenie wykluczenia musi automatycznie rozwiązywać alarmy, które pasują do utworzonego wykluczenia.
95. Kryteria wykluczeń muszą być konfigurowane w oparciu o przynajmniej: nazwę procesu, ścieżkę procesu, wiersz polecenia, wydawcę, typ podpisu, SHA-1, nazwę komputera, grupę, użytkownika.
96. Serwer musi posiadać ponad 900 wbudowanych reguł, po których wystąpieniu, nastąpi wyzwolenie alarmu bezpieczeństwa. Administrator musi też posiadać możliwość utworzenia własnych reguł i edycji reguł dodanych przez producenta.
97. Serwer administracyjny musi oferować możliwość blokowania plików po sumach kontrolnych. W ramach blokady musi istnieć możliwość dodania komentarza oraz konfiguracji wykonywanej czynności, po wykryciu wprowadzonej sumy kontrolnej.
98. Administrator musi posiadać możliwość weryfikacji uruchomionych plików wykonywalnych na stacji roboczej z możliwością podglądu szczegółów wybranego procesu przynajmniej o: SHA-1, typ podpisu, wydawcę, opis pliku, wersję pliku, nazwę firmy, nazwę produktu, wersję produktu, oryginalną nazwę pliku, rozmiar pliku oraz reputację i popularność pliku.
99. Administrator, w ramach plików wykonywalnych oraz plików DLL, musi posiadać możliwość ich oznaczenia jako bezpieczne, pobrania do analizy oraz ich zablokowania.
100. Administrator musi posiadać możliwość weryfikacji uruchomionych skryptów na stacjach roboczych, wraz z informacją dotyczącą parametrów uruchomienia. Administrator musi posiadać możliwość oznaczenia skryptu jako bezpieczny lub niebezpieczny.
101. W ramach przeglądania wykonanego skryptu, administrator musi posiadać możliwość szczegółowego podglądu wykonanych przez skrypt czynności w formie tekstowej.
102. W ramach przeglądania wykonanego skryptu lub pliku exe, administrator musi posiadać możliwość weryfikacji powiązanych zdarzeń dotyczących przynajmniej: modyfikacji plików i rejestru, zestawionych połączeń sieciowych i utworzonych plików wykonywalnych.
103. Serwer administracyjny musi oferować możliwość przekierowania do konsoli zarządzającej produktu antywirusowego tego samego producenta, w celu weryfikacji szczegółów wybranej stacji roboczej. W konsoli zarządzającej produktu antywirusowego, administrator musi mieć możliwość podglądu informacji dotyczących przynajmniej: podzespołów zarządzanego komputera (w tym przynajmniej: producent, model, numer seryjny, informacje o systemie, procesor, pamięć RAM, wykorzystanie dysku twardego, informacje o wyświetlaczu, urządzenia peryferyjne, urządzenia audio, drukarki, karty sieciowe, urządzenia masowe) oraz wylistowanie zainstalowanego oprogramowania firm trzecich.
104. Konsola administracyjna musi mieć możliwość tagowania obiektów.
105. Konsola administracyjna musi umożliwiać połączenie się do stacji roboczej z możliwością wykonywania poleceń powershell.

## II. SYSTEM OCHRONY PRZED WYCIEKAMI DLP

Niniejsza specyfikacja określa wymagania dotyczące zakupu i wdrożenia systemu Data Loss Prevention (DLP) dla Zleceniodawcy. Celem jest zapewnienie kompleksowej ochrony przed wyciekiem danych wrażliwych, poufnych informacji oraz danych osobowych, zarówno w formie strukturalnej, jak i niestukturalnej. System DLP ma na celu monitorowanie, wykrywanie, zapobieganie oraz raportowanie wszelkich nieautoryzowanych prób przesyłania, kopiowania lub udostępniania danych poza organizację, zarówno poprzez kanały elektroniczne, jak i fizyczne. Dodatkowo, system DLP ma umożliwić kontrolę nad przepływem informacji w ramach organizacji, zapewniając zgodność z obowiązującymi przepisami prawa oraz wewnętrznymi politykami bezpieczeństwa.

**Ilość licencji: 25 na okres 24 miesięcy**

**Minimalny zakres jaki musi spełniać dostarczony sprzęt/oprogramowanie:**

### 1. System operacyjny:

- a) Windows 10 (64-bit) z wszystkimi aktualizacjami zabezpieczającymi
- b) Windows 11 (64-bit) z wszystkimi aktualizacjami zabezpieczającymi
2. Serwer administracyjny musi obsługiwać instalację na systemach: a. Windows Server 2016 (64-bit) i nowszych.
3. Serwer administracyjny musi obsługiwać bazy danych: a. MS SQL Server 2016 lub nowsze, b. MS SQL Express
4. Pomoc i dokumentacja programu dostępne w języku angielskim.
5. Konsola administracyjna i komunikaty klienta muszą być w języku polskim.
6. Konsola zarządzająca musi umożliwiać pobranie pliku instalacyjnego agenta.
7. Serwer administracyjny musi umożliwiać instalację/deinstalację zdalnego klienta na stacjach roboczych.
8. Reguły DLP muszą być egzekwowane nawet przy braku połączenia między klientem a serwerem zarządzającym.
9. Brak połączenia klienta z serwerem zarządzającym musi umożliwiać lokalne przechowywanie informacji i zebranych danych do czasu ponownego połączenia.
10. Serwer administracyjny musi umożliwiać zarządzanie za pośrednictwem konsoli.
11. Administrator musi mieć możliwość konfiguracji automatycznej konserwacji dla bazy danych, usuwając najstarsze informacje, gdy rozmiar bazy osiągnie skonfigurowany limit.
12. Serwer administracyjny musi automatycznie pobierać aktualizacje definicji kategoryzowania stron internetowych, aplikacji i rozszerzeń plików, z opcją wyłączenia automatycznego pobierania.
13. Administrator musi mieć możliwość aby tworzyć, usuwać i konta administratorów w konsoli programu.
14. Administrator musi mieć możliwość przypisywania i odbierania uprawnień do wybranych modułów programu, podzielonych na ustawienia (konfiguracja modułu) i logi (wyświetlanie logów modułu).
15. Serwer musi synchronizować użytkowników i stacje robocze z domeną Active Directory.
16. System musi rejestrować zdarzenia aktywności stacji roboczej, takie jak logowanie, wylogowanie, włączenie, wyłączenie, blokada, odblokowanie i przejście w stan bezczynności.



17. Administrator musi móc wymusić synchronizację ustawień i logów między stacją roboczą a serwerem w czasie rzeczywistym.
18. Serwer administracyjny musi umożliwiać ustawienie powiadomień dla użytkownika końcowego w przypadku złamania reguł związanych z ochroną DLP, z możliwością dostosowania grafiki, adresu e-mail i odnośnika do polityki bezpieczeństwa.
19. Administrator musi mieć możliwość wykonać audyt stacji roboczych/użytkowników w oparciu o różne czynności, takie jak uruchomione aplikacje, podłączone urządzenia, odwiedzane strony internetowe, wydrukowane dokumenty, wysyłane i odebrane wiadomości e-mail oraz czynności na plikach.
20. Administrator musi mieć możliwość tworzenia własnych kategorii dla stron internetowych, aplikacji i typów plików.
21. Administrator musi mieć możliwość filtrowania i sortowania zebranych danych.
22. Serwer musi posiadać możliwość wysyłania alertów, przynajmniej za pośrednictwem wiadomości email.
23. Dashboardy muszą być generowane na podstawie wskazanych stacji roboczych, użytkowników lub grup w określonym przedziale czasu.
24. Serwer administracyjny musi posiadać wbudowany serwer SMTP dostarczony przez producenta oprogramowania.
25. Serwer administracyjny musi umożliwiać wykonywanie zadań kategoryzacji plików, zarówno istniejących na stacjach roboczych i zasobach sieciowych, jak i nowo powstałych na bazie już skategoryzowanych plików.
26. Serwer administracyjny musi mieć możliwość kategoryzacji plików wrażliwych na podstawie aplikacji, lokalizacji, adresu URL, formatu pliku i zawartości pliku.
27. Administrator musi mieć możliwość wyszukiwania danych osobowych na zasobach zarówno lokalnych, jak i sieciowych.
28. Dla plików skategoryzowanych, wymagana jest możliwość tworzenia reguł dotyczących blokowania i zezwalania na różne operacje, takie jak zapisywanie, przenoszenie, drukowanie, wysyłanie pocztą, wysyłanie do chmury, przesyłanie komunikatorami itp.
29. Serwer administracyjny musi umożliwiać wyszukiwanie i ochronę plików w oparciu o różne kryteria, takie jak numery kart kredytowych, numer PESEL, numer dowodu osobistego, numer paszportu, wyrażenia regularne, określone ciągi znaków i numer IBAN.
30. Weryfikacja zawartości pliku musi odbywać się w czasie rzeczywistym.
31. Serwer administracyjny musi pozwalać na eksport logów do rozwiązania SIEM.
32. Konsola musi umożliwiać konfigurację/zmianę domyślnego serwera SMTP.
33. Konsola webowa musi pozwalać na weryfikację wersji zainstalowanego oprogramowania klienta, a także umożliwia aktualizację do nowej wersji lub dezaktywację tego oprogramowania.
34. System musi ochraniać pocztę e-mail Microsoft 365, sprawdzając każdą wiadomość e-mail wysłaną przez użytkowników Microsoft 365.
35. System musi ochraniać pliki w Microsoft 365, kontrolując aktywność plików w Microsoft SharePoint, Microsoft OneDrive dla Firm i Microsoft Teams.
36. System musi wykorzystywać mechanizm OCR (optical character recognition), aby wykrywać poufne treści w obrazach, zdjęciach i zeskanowanych dokumentach

### III. LICENCJA NA SUBSKRYPCJĘ ZABEZPIECZEŃ TYPU IDS, IPS

Niniejsza specyfikacja określa wymagania dotyczące zakupu i wdrożenia urządzenia UTM (Unified Threat Management) dla Zleceniodawcy. Celem jest zapewnienie scentralizowanego, niezawodnego i wydajnego rozwiązania do ochrony sieci firmowej przed zagrożeniami zewnętrznymi oraz zarządzania jej bezpieczeństwem. Urządzenie UTM ma integrować

**Dostawa sprzętu sieciowego i oprogramowania na potrzeby Gminy Cielądz  
w ramach programu "Cyberbezpieczny Samorząd"**

Or.SO.2714.13.2024

różnorodne funkcje zabezpieczeń sieciowych, takie jak zaporę sieciową (firewall), system zapobiegania włamaniom (IPS), ochrona przed atakami DDoS, filtrowanie ruchu internetowego, ochrona antywirusowa, antyspamowa oraz zarządzanie sieciami VPN.

Urządzenie UTM ma umożliwiać kompleksową ochronę sieci, monitorowanie ruchu oraz zarządzanie politykami bezpieczeństwa z centralnego punktu. Dodatkowo, powinno oferować zaawansowane funkcje, takie jak kształtowanie ruchu (QoS), zarządzanie przepustowością, równoważenie obciążenia (load balancing), oraz szczegółowe raportowanie stanu bezpieczeństwa sieci. Urządzenie UTM ma także wspierać integrację z istniejącymi infrastrukturami sieciowymi, zapewniając wsparcie dla protokołów IPv4 i IPv6, wirtualne sieci prywatne (VPN) oraz zdalne zarządzanie poprzez bezpieczne połączenia.

**Planowane jest zakupienie dwóch urządzeń o różnych parametrach wraz z licencjami oraz dodatkowo samej licencji na urządzenie które jest już w posiadaniu Zamawiającego.**

#### **URZĄDZENIE TYP 1 - Ilość: 1 szt.**

##### **Minimalny zakres jaki musi spełniać dostarczony sprzęt/oprogramowanie:**

1. Obsługa sieci: Wsparcie dla IPv4 i IPv6, obsługa interfejsów, routing, firewall, systemu IPS, DHCP
2. Firewall: Stateful Inspection, translacja NAT n:1, NAT 1:1, PAT, tryb pracy router/bridge/hybrydowy
3. Reguły firewall: Konfiguracja reguł na podstawie IP, DSCP, interfejsów, usług, użytkowników LDAP, reputacji hosta, geolokacji
4. IPS (Intrusion Prevention System): Wykrywanie i prewencja ataków, własne sygnatury, inspekcja ruchu SSL, ochrona przed SQL Injection, XSS, Web2.0
5. Kształtowanie pasma: Priorytetyzacja ruchu, limity pasma dla IP, DSCP, użytkownika, monitorowanie ruchu, śledzenie typu ruchu
6. Ochrona antywirusowa: Co najmniej dwa skanery antywirusowe, możliwość konfiguracji analizy plików, komunikaty o infekcjach
7. Ochrona antyspam: Klasyfikacja SPAM oparta o białe/czarne listy, DNS RBL, heurystyczny skaner, format zgodny z Spamassassin
8. VPN: Obsługa VPN client-to-site, site-to-site (PPTP, IPSec, SSL), VPN Failover, tunelowanie SSL VPN
9. Filtr URL: Co najmniej 50 kategorii, dodawanie własnych kategorii, blokowanie MIME, filtrowanie HTTPS, SafeSearch
10. Uwierzytelnianie: LDAP, Active Directory, captive portal, wsparcie VDI, 2FA TOTP
11. Równoważenie obciążenia ISP: Load Balancing na podstawie adresu źródłowego lub połączenia, Failover, SD-WAN
12. Routing: Statyczne i dynamiczne trasowanie (RIPv2, OSPF, BGP), Policy Based Routing, obsługa IPv6
13. Administracja urządzeniem: Polski interfejs graficzny, dostęp HTTP/HTTPS, zarządzanie przez SSH, diagnostyka (ping, traceroute, nslookup), polityki haseł, backup konfiguracji, IPFIX
14. Raportowanie: System raportowania (min. 25 raportów), predefiniowane raporty dla WEB, IPS, Antywirus, Antyspam, eksport do CSV, integracja z SNMP
15. Serwer DHCP: Wbudowany serwer DHCP, DHCP Relay, wsparcie dla IPv4 i IPv6, różne konfiguracje DHCP
16. Open API: Implementacja Open API
17. Gwarancja: 12 miesięcy gwarancji na sprzęt i licencje

18. Parametry sprzętowe: Brak dysku twardego, działanie na pamięci flash, min. 8 portów Ethernet 10/100/1000 Mbps, przepustowość firewall 4Gbps, IPS 2.4Gbps, tunel VPN AES 600Mbps
19. Maksymalna liczba sesji: Min. 300 000 równoczesnych sesji, 18 000 nowych sesji/sek.
20. Klastry wysokiej dostępności (HA): Budowa klastrów HA w trybie Active-Passive
21. Liczba reguł filtrowania: Min. 8192 reguły
22. Liczba tras routingu: Min. 512 tras statycznych, 10 000 tras dynamicznych
23. Zakupione urządzenie musi być wyposażone w aktywną licencję producenta

**URZĄDZENIE TYP 2 - Ilość: 1 szt.****Minimalny zakres jaki musi spełniać dostarczony sprzęt/oprogramowanie:**

1. Obsługa sieci: Wsparcie dla IPv4 i IPv6, konfiguracja adresów, routingu, firewall, system IPS, DHCP
2. Firewall: Stateful Inspection, translacja NAT n:1, NAT 1:1, PAT, tryby router, bridge, hybrydowy, możliwość tworzenia reguł firewall
3. Reguły firewall: Min. 10 niezależnych zestawów reguł, konfiguracja na podstawie IP, DSCP, interfejsów, usług, użytkowników LDAP
4. IPS (Intrusion Prevention System): Wbudowany w jądro systemu IPS, zabezpieczenie przed min. 10 000 ataków, możliwość tworzenia własnych sygnatur, inspekcja SSL, ochrona przed SQL Injection
5. Kształtowanie pasma: Priorytetyzacja ruchu, limity pasma dla IP, DSCP, użytkowników, monitorowanie typu ruchu
6. Ochrona antywirusowa: Co najmniej dwa skanery antywirusowe, możliwość określenia maks. wielkości pliku do analizy
7. Ochrona antyspam: Mechanizmy klasyfikacji poczty oparte na białych/czarnych listach, DNS RBL, heurystyczny skaner
8. VPN: Obsługa VPN (client-to-site, site-to-site), PPTP, IPSec, SSL, VPN Failover
9. Filtr URL: Co najmniej 50 kategorii, możliwość dodawania własnych kategorii, blokowanie MIME, filtrowanie HTTPS
10. Uwierzytelnianie: LDAP, Active Directory, captive portal, wsparcie VDI, 2FA TOTP
11. Routing: Statyczne i dynamiczne trasowanie (RIPv2, OSPF, BGP), Policy Based Routing
12. Administracja urządzeniem: Polski interfejs graficzny, dostęp HTTP/HTTPS, zarządzanie przez SSH, diagnostyka (ping, traceroute, nslookup), polityki haseł, backup konfiguracji, IPFIX
13. Raportowanie: System raportowania z predefiniowanymi raportami dla WEB, IPS, Antywirus, Antyspam, min. 25 raportów, eksport do CSV
14. Serwer DHCP: Wbudowany serwer DHCP, DHCP Relay, wsparcie dla IPv4 i IPv6, różne konfiguracje DHCP
15. Open API: Implementacja Open API
16. Gwarancja: 12 miesięcy gwarancji na sprzęt i licencje
17. Parametry sprzętowe: Min. 5 portów Ethernet 10/100/1000Mbps, przepustowość firewall 1Gbps, IPS 1Gbps, VPN AES 200Mbps, obsługa do 50 tuneli IPSec, min. 150 000 sesji równoczesnych
18. Liczba reguł filtrowania: Min. 4096 reguł
19. Liczba tras routingu: Min. 512 tras statycznych, 1000 tras dynamicznych
20. Zakupione urządzenie musi być wyposażone w aktywną licencję producenta

**LICENCJA – 3 szt.** (Zamawiane są trzy licencje – dwie do urządzeń TYP 1 i 2 powyżej oraz jedna na urządzenie które jest już w posiadaniu Zamawiającego).

**Dostawa sprzętu sieciowego i oprogramowania na potrzeby Gminy Cielądz  
w ramach programu “Cyberbezpieczny Samorząd”**

Or.SO.2714.13.2024

Niniejsza specyfikacja określa wymagania dotyczące zakupu i wdrożenia systemu Unified Threat Management (UTM) dla Zleceniodawcy. Głównym celem jest zapewnienie zaawansowanej, zintegrowanej ochrony przed szerokim spektrum zagrożeń cybernetycznych, które mogą wpływać na bezpieczeństwo operacyjne i poufność danych. System UTM zostanie wykorzystany do ochrony infrastruktury IT przed atakami zewnętrznymi i wewnętrznymi, zapewniając jednocześnie ciągłość działania krytycznych systemów biznesowych.

Oprogramowanie UTM ma za zadanie integrować funkcje takie jak zaporę sieciową, system zapobiegania intruzjom (IPS), antywirus, filtracja treści oraz VPN, co umożliwia kompleksową ochronę zarówno dla danych w spoczynku, jak i przesyłanych w sieci. System będzie także wspierać zgodność z międzynarodowymi i krajowymi regulacjami dotyczącymi bezpieczeństwa danych, jak również z wewnętrznymi politykami bezpieczeństwa Zleceniodawcy. Dodatkowo, implementacja systemu UTM ma umożliwić efektywne zarządzanie bezpieczeństwem sieciowym, zcentralizowaną kontrolę i łatwe skalowanie w miarę rozwoju organizacji. Czas trwania wsparcia: min 2 lata. W pakiecie powinny znaleźć się następujące funkcjonalności:

1. Aktualizacje
2. Wymiana w przypadku awarii (14 dni)
3. Wsparcie techniczne
4. NGFW + IPS
5. IPSec + SSL VPN
6. Antywirus
7. Filtr URL
8. Antyspam

#### IV. OPROGRAMOWANIE SZYFRUJĄCE

Niniejsza specyfikacja określa wymagania dotyczące zakupu i wdrożenia oprogramowania szyfrującego dla Zleceniodawcy. Celem jest zapewnienie kompleksowej ochrony poufnych danych oraz informacji wrażliwych przed nieautoryzowanym dostępem, zarówno w spoczynku, jak i podczas transmisji. Oprogramowanie szyfrujące ma na celu umożliwienie bezpiecznego przechowywania danych na różnych nośnikach, takich jak dyski twarde, pamięci przenośne czy chmura obliczeniowa, a także ochronę danych przesyłanych przez sieci komputerowe, w tym Internet. Dodatkowo, oprogramowanie szyfrujące ma zapewnić zgodność z obowiązującymi przepisami prawa oraz wewnętrznymi politykami bezpieczeństwa, a także umożliwić łatwe zarządzanie kluczami szyfrującymi oraz kontrolę dostępu do zaszyfrowanych danych.

**Ilość licencji: 25 na okres 24 miesięcy**

**Minimalny zakres jaki musi spełniać dostarczony sprzęt/oprogramowanie:**

**Ochrona danych – szyfrowanie:**

1. Konsola centralnego zarządzania musi wspierać systemy operacyjne Microsoft Windows Server 2016, 2019, 2022 oraz Microsoft Windows 10 i 11.
2. Serwer centralnego zarządzania musi współpracować co najmniej z silnikami baz danych takimi jak Microsoft SQL Server 2012, 2014, 2016, 2017, 2019 w wersji przynajmniej Express.

**Dostawa sprzętu sieciowego i oprogramowania na potrzeby Gminy Cielądz  
w ramach programu “Cyberbezpieczny Samorząd”**

Or.SO.2714.13.2024

3. Konsola centralnego zarządzania musi pozwalać na generowanie pakietów instalacyjnych dla stacji końcowych w formacie MSI.
4. Komunikacja pomiędzy serwerem centralnego zarządzania, a serwerem proxy musi odbywać się na bezpiecznym porcie 443.
5. Administrator musi mieć możliwość tworzenia i zarządzania wieloma kluczami szyfrującymi, opartymi o kilka algorytmów szyfrujących, co najmniej AES, 3DES, Blowfish.
6. Administrator musi mieć możliwość tworzenia różnych użytkowników, mających dostęp do konsoli centralnego zarządzania wraz z możliwością przypisywania im różnych ról.
7. Administrator musi mieć możliwość tworzenia dodatkowych ról, na podstawie opcji dostępnych w konsoli centralnego zarządzania.
8. Logowanie do konsoli centralnego zarządzania powinno być objęte warunkami złożoności hasła.
9. Musi istnieć możliwość konfiguracji złożoności hasła do konsoli centralnego zarządzania, w oparciu o przynajmniej:
  - a) ilość znaków,
  - b) czy hasło ma zawierać wielkie litery,
  - c) czy hasło ma zawierać małe litery,
  - d) czy hasło ma zawierać cyfry,
  - e) czy hasło ma zawierać znaki specjalne,
  - f) okres ważności,
  - g) ilość nieudanych logowań.
10. Administrator musi mieć możliwość konfiguracji złożoności haseł dla użytkowników na stacjach roboczych.
11. Musi istnieć możliwość konfiguracji złożoności hasła dla użytkowników na stacjach roboczych, w oparciu o przynajmniej:
  - a) ilość znaków,
  - b) czy hasło ma zawierać wielkie litery,
  - c) czy hasło ma zawierać małe litery,
  - d) czy hasło ma zawierać cyfry,
  - e) czy hasło ma zawierać znaki specjalne,
  - f) okres ważności,
  - g) ilość nieudanych logowań,
  - h) możliwość zmiany hasła.
12. Konsola centralnego zarządzania musi gromadzić informacje o:
  - a) nazwach stacji roboczych, na których jest zainstalowany klient systemu szyfrowania danych,
  - b) dacie ostatniej modyfikacji ustawień klienta systemu szyfrowania danych,
  - c) dacie aktywacji klienta systemu szyfrowania danych,
  - d) statusu szyfrowania,
  - e) typie urządzenia na którym jest zainstalowany klient systemu szyfrowania danych,
  - f) stanie polityki,
  - g) wersji klienta systemu szyfrowania danych,



- h) wersji systemu operacyjnego stacji roboczej,
- i) użytkownikach uprawnionych do logowania do oprogramowania na stacji roboczej.
- 13. Konsola centralnego zarządzania musi pozwalać na wygenerowanie dla każdej zaszyfrowanej stacji płyty ratunkowej.
- 14. Konsola musi być dostępna z poziomu interfejsu WWW.
- 15. Administrator musi mieć możliwość zarządzania stacjami klienckimi, które mają dostęp do sieci Internet.
- 16. Administrator musi mieć możliwość konfiguracji automatycznego szyfrowania pełnej powierzchni dysku po wykonanej instalacji oprogramowania.
- 17. Konsola centralnego zarządzania musi posiadać możliwość automatycznej aktywacji licencji w ramach kont domenowych.
- 18. Administrator musi mieć możliwość wykonania poniższych czynności w sposób zdalny:
  - a) instalacji klienta na stacji,
  - b) zaszyfrowania/odszyfrowania stacji,
  - c) wygenerowania klucza aktywacyjnego dla użytkownika,
  - d) administrowania kluczami szyfrującymi,
  - e) administrowania użytkownikami, którzy mają dostęp do stacji,
  - f) administrowania profilem ustawień dla użytkowników,
  - g) administrowania profilem ustawień dla stacji roboczych,
  - h) wymuszenia zmiany hasła,
  - i) zarządzania wieloma organizacjami z poziomu jednej konsoli.

#### **Wymagania systemowe aplikacji klienckiej:**

- 19. System szyfrowania danych musi wspierać instalacje aplikacji klienckiej w środowisku Microsoft Windows 10 i 11 oraz w środowiskach Microsoft Windows Server 2012, 2012 R2, 2016, 2019, 2022.

#### **Wymagania dotyczące uwierzytelniania:**

- 20. Aplikacja musi posiadać autentykację typu Pre-boot, czyli uwierzytelnienie użytkownika zanim zostanie uruchomiony system operacyjny.
- 21. Aplikacja musi umożliwiać określenie, co najmniej 127 unikalnych użytkowników, którzy będą mieć dostęp do chronionej stacji roboczej na poziomie Pre-Boot.
- 22. Aplikacja musi umożliwiać przetrzymywanie, co najmniej 64 kluczy szyfrujących w jednym pęku kluczy (key file).
- 23. Dostęp do pliku klucza musi być chroniony przy pomocy hasła. Domyślnie wykorzystywane hasło musi być hasłem systemu Windows.
- 24. Administrator musi posiadać możliwość modyfikacji ekranu logowania (Pre-boot).

#### **Wymagania dotyczące ustawień aplikacji klienckiej:**

- 25. Aplikacja musi być dostępna, przynajmniej w języku polskim i angielskim.
- 26. Defragmentacja dysku nie może mieć negatywnego wpływu na system szyfrowania.
- 27. Aplikacja musi umożliwiać szyfrowanie nośników wymiennych w następujący sposób:
  - a) sektor po sektorze,

b) kontener.

28. Zaszyfrowany nośnik wymienny oraz nośnik CD/DVD może być odczytany na dowolnej stacji, na której nie ma zainstalowanego klienta systemu szyfrowania. Dostęp do takiego nośnika musi być możliwy po podaniu hasła.
29. Aplikacja musi pozwalać na szyfrowanie wiadomości e-mail wraz z załącznikami.
30. Aplikacja musi umożliwiać automatyczną deszyfrację otrzymywanych wiadomości e-mail.
31. Aplikacja musi pozwalać na szyfrowanie całego tekstu dokumentu, jego części, a także zawartości schowka systemowego.
32. Zaszyfrowany tekst może być odczytany, za pomocą narzędzia, dostarczanego przez producenta, na stacji bez zainstalowanego klienta systemu szyfrowania.
33. Aplikacja musi umożliwiać wybór klucza szyfrującego (w przypadku posiadania wielu kluczy w pęku), który ma być używany w procesie szyfrowania.
34. Aplikacja musi umożliwiać wybór domyślnego klucza szyfrowania.
35. Aplikacja musi umożliwiać zaszyfrowanie pliku lub folderu z poziomu menu kontekstowego.
36. Możliwe jest utworzenie skrótów klawiszowych umożliwiających zaszyfrowanie/ odszyfrowanie całego tekstu dokumentu, jego części, a także zawartości schowka systemowego.
37. Aplikacja musi umożliwiać tworzenie wirtualnych partycji. Dostęp do takich partycji ma być możliwy przy użyciu klucza szyfrującego lub hasła.
38. Aplikacja musi umożliwiać zdefiniowanie wielkości wirtualnej partycji, z dokładnością do 1MB.
39. Aplikacja musi umożliwiać tworzenie zaszyfrowanego archiwum. Dostęp do takiego archiwum ma być możliwy, przy użyciu klucza szyfrującego lub hasła.
40. Aplikacja musi umożliwiać trwałe usuwanie danych za pomocą poniższych algorytmów:
  - a) Guttman.
  - b) US Department of Defence 5220.22-M (8-306. /E).
  - c) US Department of Defence 5220.22-M (8-306. /E, CiE).
  - d) Kryptograficzne losowe dane liczbowe.
41. Aplikacja musi posiadać dedykowaną wtyczkę co najmniej dla klientów pocztowych MS Outlook 2003 lub nowszych, również dostępnych z poziomu Office 365.
42. Aplikacja musi umożliwiać automatyczne zalogowanie użytkownika do pęku klucza (key file) systemu szyfrowania danych po uruchomieniu systemu operacyjnego.
43. Aplikacja musi umożliwiać automatyczne wylogowanie z aplikacji w przypadku bezczynności użytkownika w systemie.
44. Aplikacja musi posiadać opcję automatycznego odpytywania serwerów producenta o dostępność nowszych wersji.
45. Użytkownik musi posiadać możliwość ręcznego sprawdzania czy dostępna jest nowsza wersja programu, z poziomu GUI.

#### **Wymagania dotyczące szyfrowania:**

46. Aplikacja musi dawać możliwość szyfrowania powierzchni dysku sektor po sektorze.
47. Szyfrowanie pełnej powierzchni dysku musi umożliwiać wykorzystanie modułu TPM.

48. Aplikacja musi umożliwiać wstrzymanie procesu szyfrowania powierzchni dysku i jego wznowienie. Proces szyfrowania danych powinien rozpocząć się od momentu, w którym został przerwany.
49. Aplikacja musi umożliwiać wstrzymanie procesu szyfrowania, w sytuacji gdy laptop nie jest podłączony do zasilania. Proces szyfrowania musi zostać wznowiony automatycznie, po podłączeniu zasilacza.
50. Wymagane jest wykorzystanie kluczy szyfrujących, utworzonych przy użyciu jednego z poniższych algorytmów szyfrowania:
  - a) AES (Rijndael).
  - b) Blowfish.
  - c) Triple DES (3DES).
51. Aplikacja musi umożliwiać współpracę z dyskami SSD.
52. Aplikacja musi umożliwiać współpracę z dyskami sprzętowo szyfrowanymi, działającymi w technologii TCG OPAL.
53. Aplikacja musi umożliwiać szyfrowanie danych na komputerach z UEFI.
54. Administrator musi mieć możliwość sprawdzenia, przed zaszyfrowaniem całej powierzchni dysku, czy nie pojawią się problemy po ponownym uruchomieniu komputera.
55. Administrator musi mieć możliwość opcjonalnego szyfrowania niesystemowych partycji dysku.

#### **Wymagania dotyczące sytuacji krytycznych:**

56. W przypadku utraty hasła, aplikacja musi umożliwiać Administratorowi odzyskanie dostępu do zaszyfrowanego dysku poprzez użycie zdefiniowanego wcześniej hasła administratora.
57. W przypadku utraty hasła, aplikacja musi umożliwiać użytkownikowi odzyskanie dostępu do zaszyfrowanego dysku, poprzez użycie otrzymanego od administratora jednorazowego hasła, wygenerowanego z poziomu konsoli centralnego zarządzania.

### **V. BATERIE ZEWNĘTRZNE DO PODTRZYMANIA ZASILANIA AWARYJNEGO URZĄDZEŃ SERWEROWYCH TYPU UPS**

Niniejsza specyfikacja określa wymagania dotyczące zakupu i wdrożenia systemu zasilania awaryjnego UPS (Uninterruptible Power Supply) dla Zleceniodawcy. Celem jest zapewnienie ciągłości działania i ochrony krytycznej infrastruktury IT przed zakłóceniami w dostawie prądu. System UPS ma umożliwić bezpieczne i stabilne funkcjonowanie serwerów, zapobiegając utracie danych i minimalizując ryzyko przestojów w przypadku awarii zasilania. Urządzenie UPS powinno oferować nie tylko wysoką jakość i niezawodność, ale także możliwość skalowania w miarę rozwoju infrastruktury IT Zleceniodawcy. Dodatkowo, system ma być wyposażony w zaawansowane funkcje monitorowania i zarządzania energią, umożliwiające optymalizację zużycia energii oraz automatyczne przełączanie na zasilanie awaryjne w przypadku wykrycia problemów z głównym źródłem zasilania.

**Ilość: 2 szt.**

**Minimalny zakres jaki musi spełniać dostarczony sprzęt/oprogramowanie:**

**Dostawa sprzętu sieciowego i oprogramowania na potrzeby Gminy Cielądz  
w ramach programu "Cyberbezpieczny Samorząd"**

Or.SO.2714.13.2024

### **UPS 6000VA:**

1. Moc pozorna: min. 6000VA
2. Moc rzeczywista: min. 6000W
3. Technologia: on-line (VFI), podwójna konwersja
4. Sprawność max (dla VFI): 95%
5. Typ obudowy: rack/tower

### **Praca sieciowa:**

6. zakres napięcia wejściowego: 110V – 275V
7. zakres częstotliwości napięcia wejściowego: 45 - 55 Hz / 54 - 66 Hz
8. Zakres napięcia wyjściowego: 208 V AC / 220 V AC / 230 V AC / 240 V AC -  
domyślnie 230 V AC
9. Wartość napięcia wyjściowego ustawiana z panelu LCD: tak
10. Kształt napięcia wyjściowego: sinusoidalny
11. Czas przełączania sieć – UPS: 0ms
12. Współczynnik odkształceń prądu wejściowego THDi: < 3%

### **Praca bateryjna:**

13. Napięcie wyjściowe:  $\sim 230V \pm 1\%$
14. Częstotliwość napięcia wyjściowego : 50Hz/60Hz  $\pm 0,1Hz$
15. Kształt napięcia wyjściowego na pracy bateryjnej: sinusoidalny
16. Zabezpieczenie przeciwzwarceniowe gniazd wyjściowych: Bezpiecznik automatyczny 20A
17. Zabezpieczenie przeciążeniowe: elektroniczne
18. Akumulatory w UPS: nie
19. Akumulatory w Modułach Bateriajnych: minimum 20x 12V 9Ah; szczelne, bezobsługowe
20. Czas podtrzymania dla obciążenia 5kW: minimum 25min ( przy wykorzystaniu baterii w maksymalnie 2 zewnętrznych Modułach Bateriajnych)

### **Pozostałe:**

21. Przeciężalność:  
100% < obciążenie  $\leq 105\%$ : ciągłe  
105% < obciążenie  $\leq 125\%$ : 10 minut  
125% < obciążenie  $\leq 150\%$ : 30s  
>150% : 500ms
22. Wejście zasilania: Listwa zaciskowa
23. Ilość i typ gniazd wyjściowych: W UPS minimum 2x IEC 320 C13 (10 A) niesterowalne + listwa zaciskowa
24. Sygnalizacja: Wyświetlacz LCD (informacje wskazujące pracę sieciową, baterijną, przeciążenie i ładowanie akumulatora). Diody LED
25. Możliwość podłączenia dodatkowych, zewnętrznych modułów bateryjnych: Wymagana możliwość podłączenia minimum 5 zewnętrznych modułów bateryjnych
26. Interfejs komunikacyjny: RS232, USB HID, karta SNMP/http -opcja
27. Złącze EPO: wymagane
28. Styki bezpotencjałowe zamontowane na stałe w obudowie UPS: wymagany minimum 1x wejściowy i 1x wyjściowy
29. Wsporniki do montażu w szafie RACK: wymagane

30. Waga UPSa: do 14,5 kg
31. Waga pojedynczego MODUŁU BATTERYJNEGO: do 69 kg
32. Wymiary UPS - wersja RACK: nie większe niż: wysokość 86mm; szerokość 438mm; głębokość 576mm
33. Wymiary MODUŁ BATTERYJNY - wersja RACK: nie większe niż: wysokość 130mm; szerokość 438mm; głębokość 596mm
34. Łączna wysokość w szafie RACK 19" dla oferowanego zestawu: nie więcej niż 8U

**Oprogramowanie:**

35. Bezpłatne oprogramowanie tego samego producenta co UPS, w języku polskim do zarządzania i monitorowania pracy UPS dla Windows, Linux oraz systemów wirtualizacji VMware, Hyper-V, Citrix XenServer bez ograniczeń co do ilości monitorowanych stanowisk (bez dodatkowych opłat za licencje)
36. Możliwość edycji nazw urządzeń na liście monitorowanych UPSów
37. Wymagane wsparcie producenta (telefoniczne oraz mailowe) w języku polskim odnośnie konfiguracji i rozwiązywania problemów.

**Gwarancja oraz serwis:**

38. Gwarancja: minimum 12 miesięcy na elektronikę i 12 miesięcy na akumulatory (opcjonalnie 24 miesiące na elektronikę i 24 miesiące na akumulatory – zgodnie z kryteriami oceny ofert);
39. Serwis: autoryzowany serwis producenta zlokalizowany w Polsce. Naprawa w maksymalnie 5 dni roboczych. Serwis realizowany w systemie door to door (opcjonalnie – zgodnie z kryteriami oceny ofert).
40. Certyfikaty producenta ISO 9001:2015 dla producenta sprzętu obejmujący proces projektowania, produkcji i serwisowania lub równoważne; deklaracja CE producenta sprzętu lub równoważne

**VI. SIECIOWE URZĄDZENIE PRZECHOWYWANIA DANYCH TYPU NAS**

Niniejsza specyfikacja określa wymagania dotyczące zakupu i wdrożenia urządzenia NAS (Network Attached Storage) dla Zleceniodawcy. Celem jest zapewnienie scentralizowanego, niezawodnego i wydajnego rozwiązania do przechowywania oraz udostępniania danych w sieci lokalnej. Urządzenie NAS ma umożliwić bezpieczne przechowywanie plików, kopii zapasowych, multimediów oraz innych danych cyfrowych, a także zapewnić dostęp do nich z różnych urządzeń, takich jak komputery, laptopy, smartfony czy tablety. Dodatkowo, urządzenie NAS ma oferować możliwość rozbudowy pojemności, redundantne dyski twarde dla zapewnienia bezpieczeństwa danych oraz zaawansowane funkcje, takie jak synchronizacja plików, strumieniowanie multimediów czy hosting aplikacji.

**Ilość: 1 szt.**

**Minimalny zakres jaki musi spełniać dostarczony sprzęt/oprogramowanie:**

1. Specyfikacja sprzętowa
2. Procesor: Procesor 64 bit Intel x86 o bazowym taktowaniu nie mniejszym niż 2.0 GHz
3. Procesor liczba rdzeni: Nie mniej niż 4
4. Pamięć RAM: Nie mniej niż 8 GB

**Dostawa sprzętu sieciowego i oprogramowania na potrzeby Gminy Cielądz  
w ramach programu “Cyberbezpieczny Samorząd”**

Or.SO.2714.13.2024



5. Pamięć Flash: Nie mniej niż 4GB
6. Liczba zatok na dyski twarde: Minimum 4
7. Obsługiwane dyski twarde: 3.5" oraz 2.5" SATA oraz 2.5" SATA SSD
8. Pojemność dysków twardych: możliwość stosowania dysków o pojemnościach do 22TB
9. Możliwość podłączenia modułu rozszerzającego: Tak, co najmniej 2
10. Porty LAN 2,5 GbE: Minimum 2
11. Diody LED: Minimum Status, LAN, HDD,
12. Porty USB 3.2 Gen 2: Minimum 2
13. Porty USB 2.0: Minimum 2
14. Port PCIe: Tak, minimum 1 Gen3
15. Przyciski: Reset, Zasilanie
16. Typ obudowy: RACK, 1U
17. Dopuszczalna temperatura pracy: od 0 do 40°C
18. Wilgotność względna podczas pracy: 5-95% R.H.
19. Zasilanie: Zasilacz redundatny max. 2 x 250 W, 100-240 V
20. Specyfikacja oprogramowania:
21. Agregacja łączy: Tak
22. Obsługiwane systemy plików: Dyski wewnętrzne: EXT4, Dyski zewnętrzne: EXT3, EXT4, NTFS, FAT32, HFS+
23. Szyfrowanie wolumenów: Tak, min AES 256
24. Szyfrowanie dysków zewnętrznych: Tak
25. Zarządzanie dyskami:
  - Pojedynczy Dysk, 0, 1, 5, 6, 10, JBOD,
  - Obsługa Hot Spare per grupa RAID oraz global hot spare
  - Rozszerzanie pojemności Online RAID
  - Migracja poziomów Online RAID
  - HDD S.M.A.R.T.
  - Skanowanie uszkodzonych bloków (pliku)
  - Przywracanie macierzy RAID
  - Obsługa map bitowych
  - Pula pamięci masowej
  - Obsługa migawek
  - Obsługa replikacji migawek
26. Zarządzanie dyskami:
  - Pojedynczy Dysk, 0, 1, 5, 6, 10, JBOD,
  - Obsługa Hot Spare per grupa RAID oraz global hot spare
  - Rozszerzanie pojemności Online RAID
  - Migracja poziomów Online RAID
  - HDD S.M.A.R.T.
  - Skanowanie uszkodzonych bloków (pliku)
  - Przywracanie macierzy RAID
  - Obsługa map bitowych
  - Pula pamięci masowej
  - Obsługa migawek
  - Obsługa replikacji migawek
27. Wbudowana obsługa iSCSI:
  - Multi-LUNs na Target
  - Obsługa LUN Mapping & Masking

- Obsługa SPC-3 Persistent Reservation
  - Obsługa MPIO & MC/S, Migawka / kopia zapasowa iSCSI LUN
28. Zarządzanie prawami dostępu:
- Ograniczenie dostępnej pojemności dysku dla użytkownika
  - Importowanie listy użytkowników
  - Zarządzanie kontami użytkowników
  - Zarządzanie grupą użytkowników
  - Zarządzanie współdzieleniem w sieci
  - Tworzenie użytkowników za pomocą makr
  - Obsługa zaawansowanych uprawnień dla podfolderów, Windows ACL
29. Obsługa Windows AD:
- Logowanie użytkowników poprzez CIFS/SMB, AFP, FTP oraz menadżera plików sieci Web
  - Funkcja serwera LDAP
30. Funkcje backup: Oprogramowanie do tworzenia kopii bezpieczeństwa producenta urządzenia dla systemów Windows, backup na zewnętrzne dyski twarde.
31. Współpraca z zewnętrznymi dostawcami usług chmury: Przynajmniej: Google Drive, Dropbox, Microsoft OneDrive, Microsoft OneDrive for Business i Box
32. Darmowe aplikacje na urządzenia mobilne:
- Monitoring / Zarządzanie / Współdzielenie plików / obsługa kamer / Odtwarzacz muzyki
  - Dostępne na systemy iOS oraz Android
33. Minimum obsługiwane serwery:
- Serwer plików
  - Serwer FTP
  - Serwer WEB
  - Serwer kopii zapasowych
  - Serwer multimediiów UPnP
  - Serwer pobierania (Bittorrent / HTTP / FTP)
  - Serwer Monitoringu
34. VPN: VPN client / VPN server. Obsługa PPTP, OpenVPN
35. Administracja systemu:
- Połączenia HTTP/HTTPS
  - Powiadamianie przez e-mail (uwierzytelnianie SMTP)
  - Powiadamianie przez SMS
  - Ustawienia inteligentnego chłodzenia
  - DDNS oraz zdalny dostęp w chmurze
  - SNMP (v2 & v3)
  - Obsługa UPS z zarządzaniem SNMP (USB)
  - Obsługa sieciowej jednostki UPS
  - Monitor zasobów
  - Kosz sieciowy dla CIFS/SMB oraz AFP
  - Monitor zasobów systemu w czasie rzeczywistym
  - Rejestr zdarzeń
  - System plików dziennika
  - Całkowity rejestr systemowy (poziom pliku)
  - Zarządzanie zdarzeniami systemowymi, rejestr, bieżące połączenie użytkowników on-line

- Aktualizacja oprogramowania
  - Kopia zapasowa ustawień/przywracanie ustawień/resetowanie ustawień systemu
36. Wirtualizacja:
- Wbudowana aplikacja umożliwiająca tworzenie środowiska wirtualnego wraz z instalacją maszyn wirtualnych na systemach Windows, Linux i Android.
  - Dostęp do konsoli maszyn za pośrednictwem przeglądarki z HTML5
  - Funkcjonalności importu, eksportu, klonowania i wykonywania migawek maszyn wirtualnych.
37. Konteneryzacja: Możliwość uruchomienia wirtualnych kontenerów dla LXC i Docker
38. Zabezpieczenia:
- Filtracja IP
  - Ochrona dostępu do sieci z automatycznym blokowaniem
  - Połączenie HTTPS
  - FTP z SSL/TLS (Explicit)
  - Obsługa SFTP
  - Szyfrowanie AES 256-bit
  - Szyfrowana zdalna replikacja (Rsync poprzez SSH)
  - Import certyfikatu SSL
  - Powiadomienia o zdarzeniach za pośrednictwem Email i SMS
39. Możliwość instalacji dodatkowego oprogramowania: Tak, sklep z aplikacjami; możliwość instalacji z paczek
40. Gwarancja: 2 lata

## VII. SERWER

Niniejsza specyfikacja określa wymagania dotyczące zakupu i wdrożenia serwerowego urządzenia dla Zamawiającego. Celem jest zapewnienie scentralizowanej, niezawodnej i wydajnej platformy serwerowej, która umożliwi hostowanie aplikacji, usług oraz przechowywanie danych. Urządzenie serwerowe ma wspierać zarządzanie bazami danych, hosting stron internetowych, wirtualizację oraz przetwarzanie danych na wysokim poziomie. Serwer powinien zapewniać skalowalność, wydajność, a także bezpieczeństwo, umożliwiając pracę w środowisku wielozadaniowym oraz zarządzanie wieloma użytkownikami i aplikacjami jednocześnie.

Dodatkowo, serwer ma oferować możliwość rozbudowy zasobów obliczeniowych (procesory, pamięć RAM), pojemności dyskowej oraz systemów redundancji, takich jak RAID, w celu ochrony danych. Urządzenie powinno być wyposażone w zaawansowane systemy chłodzenia, zasilania awaryjnego oraz monitorowania wydajności i stanu urządzenia, zapewniając tym samym ciągłość pracy w trybie 24/7.

**Ilość: 2 (1x TYP 1 oraz 1x TYP 2)**

### Minimalne wymagane parametry - TYP 1:

#### Obudowa:

1. Obudowa serwerowa do montażu w szafie RACK 19" wraz z wysuwanymi szynami dedykowanymi do tego urządzenia przez producenta serwera.
2. Obudowa powinna posiadać wpanel LCD pozwalający jednoznacznie stwierdzić czy system działa poprawnie i pokazujący podstawowe stany działania serwera.

**Dostawa sprzętu sieciowego i oprogramowania na potrzeby Gminy Cielądz  
w ramach programu "Cyberbezpieczny Samorząd"**

Or.SO.2714.13.2024

3. W obudowie powinien być zainstalowany zestaw redundantnych zasilaczy o mocy co najmniej 1100W w standardzie Titanium każdy wymiennalny podczas pracy
4. Zestaw redundantnych wentylatorów. Wentylatory powinny mieć możliwość wymiany podczas pracy systemu
5. Wbudowany czujnik otwarcia obudowy współpracujący z BIOS i kartą zarządzającą.
6. Obudowa powinna posiadać możliwość instalacji interfejsu NFC do połączenia z aplikacją zarządzającą serwerem na telefonie.
7. Aplikacja zarządzająca powinna być dostępna na Android i iOS

#### **Płyta główna:**

7. Obsługująca co najmniej dwa procesory i co najmniej 16 slotów na pamięć taktowaną przynajmniej z częstotliwością 3200MT/s przy użyciu odpowiednich procesorów.
8. musi być zaprojektowana przez producenta serwera i oznaczona jego znakiem firmowym musi być wyposażona w zaimplementowane sprzętowo mechanizmy kryptograficzne poświadczające integralność oprogramowania BIOS (Root of Trust),
9. Musi umożliwiać utworzenie bezpiecznego profilu w oparciu o konfigurację sprzętową oraz o konfigurację wewnętrznego oprogramowania komponentów serwera.
10. Zintegrowany z płytą główną moduł TPM w wersji co najmniej 2.0

#### **Procesor:**

11. Procesor typu skalowalnego z uwagi na licencjonowanie posiadający dokładnie 8 rdzeni działający co najmniej z częstotliwością 2.8GHz i dający w teście Passmark dostępnym na stronie <https://www.cpubenchmark.net/> wynik nie mniejszy niż 19010

#### **Pamięć RAM:**

12. 64 GB pamięci RAM w modułach 32GB RDIMM przygotowanych na działanie z częstotliwością co najmniej 3200MT/s

#### **Dyski:**

13. Miejsce na co najmniej 12 dysków w rozmiarze 3.5" wymiennalne bez wyłączania systemu.
14. Serwer ma mieć przewidzianą przez producenta możliwość dodania modułu pozwalającego na startowanie systemu z kart SD lub dysków M.2 skonfigurowanych w RAID1 nie zajmujących slotów na dyski.
15. Serwer powinien posiadać kontroler RAID umożliwiający konfigurację RAID 0, 1, 5, 10, 50, 6 posiadający co najmniej 8GB pamięci cache zabezpieczonej przed awarią prądu.
16. W serwerze powinny być zainstalowane co najmniej dwa dyski co najmniej 480GB SSD skonfigurowane fabrycznie w RAID 1 oraz trzy dyski co najmniej 4TB co najmniej NLSAS 12Gbps

#### **Karta sieciowa:**

17. Na płycie głównej powinna być zainstalowana dwuportowa karta sieciowa 1GB BT
18. Karta nie może zajmować slotu PCIe
19. Dwuportowa karta sieciowa 10GB BT
20. Karta nie może zajmować slotu PCIe
21. Dodatkowo w serwerze powinna być zainstalowana czteroportowa karta sieciowa 1GB BT

**Karta zarządzająca:**

22. Niezależna od zainstalowanego na serwerze systemu operacyjnego posiadająca dedykowane port RJ-45 Gigabit Ethernet umożliwiające:
23. zdalny dostęp do graficznego interfejsu Web karty zarządzającej
24. szyfrowane połączenie (TLS) oraz autentykację i autoryzację użytkownika
25. możliwość podmontowania zdalnych wirtualnych napędów
26. wirtualną konsolę z dostępem do myszy, klawiatury
27. wsparcie dla IPv6 - wsparcie dla SNMP; IPMI2.0, VLAN tagging, SSH
28. możliwość zdalnego monitorowania w czasie rzeczywistym poboru prądu przez serwer, dane historyczne powinny być dostępne przez min. 7 dni wstecz.
29. możliwość zdalnego ustawienia limitu poboru prądu przez konkretny serwer
30. integracja z Active Directory
31. możliwość obsługi przez ośmiu administratorów jednocześnie
32. Wsparcie dla automatycznej rejestracji DNS - wsparcie dla LLDP
33. wysyłanie do administratora maila z powiadomieniem o awarii lub zmianie konfiguracji sprzętowej
34. możliwość podłączenia lokalnego poprzez złącze RS-232.
35. możliwość zarządzania bezpośredniego poprzez złącze microUSB umieszczone na froncie obudowy.
36. Monitorowanie zużycia dysków SSD
37. możliwość monitorowania z jednej konsoli min. 100 serwerami fizycznymi,
38. Automatyczne zgłaszanie alertów do centrum serwisowego producenta
39. Automatyczne update firmware dla wszystkich komponentów serwera
40. Możliwość przywrócenia poprzednich wersji firmware
41. Możliwość eksportu eksportu/importu konfiguracji (ustawienie karty zarządzającej, BIOSu, kart sieciowych, HBA oraz konfiguracji kontrolera RAID) serwera do pliku XML lub JSON
42. Możliwość zaimportowania ustawień, poprzez bezpośrednie podłączenie plików konfiguracyjnych
43. Automatyczne tworzenie kopii ustawień serwera w oparciu o harmonogram.

**Oprogramowanie zarządzające:**

44. wsparcie dla serwerów, urządzeń sieciowych oraz pamięci masowych;
45. możliwość zarządzania dostarczonymi serwerami bez udziału dedykowanego agenta;
46. wsparcie dla protokołów – WMI, SNMP, IPMI, WSMAN, Linux SSH;
47. możliwość oskryptowywania procesu wykrywania urządzeń;
48. możliwość uruchamiania procesu wykrywania urządzeń w oparciu o harmonogram;
49. szczegółowy opis wykrytych systemów oraz ich komponentów;
50. możliwość eksportu raportu do CSV, HTML, XLS;
51. grupowanie urządzeń w oparciu o kryteria użytkownika;
52. automatyczne skrypty CLI umożliwiające dodawanie i edycję grup urządzeń;
53. szybki podgląd stanu środowiska;
54. podsumowanie stanu dla każdego urządzenia;
55. szczegółowy status urządzenia/elementu/komponentu;
56. generowanie alertów przy zmianie stanu urządzenia;
57. filtry raportów umożliwiające podgląd najważniejszych zdarzeń;



58. integracja z service desk producenta dostarczonej platformy sprzętowej;
59. możliwość przejęcia zdalnego pulpitu;
60. możliwość podmontowania wirtualnego napędu;
61. kreator umożliwiający dostosowanie akcji dla wybranych alertów;
62. możliwość importu plików MIB;
63. przesyłanie alertów „as-is” do innych konsol firm trzecich;
64. aktualizacja oparta o wybranie źródła bibliotek (lokalna, on-line producenta oferowanego rozwiązania);
65. możliwość instalacji sterowników i oprogramowania wewnętrznego bez potrzeby instalacji agenta;
66. możliwość automatycznego generowania i zgłaszania incydentów awarii bezpośrednio do centrum serwisowego producenta serwerów;
67. moduł raportujący pozwalający na wygenerowanie następujących informacji: nr seryjny sprzętu, konfiguracja poszczególnych urządzeń, wersje oprogramowania wewnętrznego, obsadzenie slotów PCIe i gniazd pamięci, informację o maszynach wirtualnych, aktualne informacje o stanie gwarancji, adresy IP kart sieciowych.

**Warunki gwarancji:**

68. 2 lata gwarancji producenta, z czasem reakcji do następnego dnia roboczego od przyjęcia zgłoszenia - zgłoszenia przyjmowane 7 dni w tygodniu w trybie 24/7.
69. Gwarancja musi obejmować całość rozwiązania nie powinno być tak aby jakaś część tego rozwiązania nie podlegała gwarancji.
70. możliwość zgłaszania awarii poprzez ogólnopolską linię telefoniczną producenta.
71. Producent musi dawać możliwość rozszerzenia gwarancji do 7 lat
72. W przypadku naprawy dysku - uszkodzony dysk zostaje u klienta.
73. Podczas trwania gwarancji producent powinien zapewnić narzędzia i procesy do proaktywnej oceny stanu technicznego oraz automatycznego zgłaszania usterek bez ingerencji człowieka.
74. Powinna być możliwość skorzystania z pomocy wsparcia producenta za pomocą komunikatora np. messenger, teams, WhatsApp.
75. Firma serwisująca musi posiadać ISO 9001:2015 na świadczenie usług serwisowych oraz posiadać autoryzację producenta urządzeń lub równoważne.
76. Możliwość sprawdzenia statusu gwarancji poprzez stronę producenta podając unikatowy numer urządzenia oraz pobieranie uaktualnień mikrokodu oraz sterowników nawet w przypadku wygaśnięcia gwarancji serwera
77. Możliwość telefonicznego sprawdzenia konfiguracji sprzętowej serwera oraz warunków gwarancji po podaniu numeru seryjnego bezpośrednio u producenta lub jego przedstawiciela.

**Certyfikaty:**

78. Serwer musi być wyprodukowany zgodnie z normą ISO-9001:2015 lub równoważną oraz ISO-14001 lub równoważną
79. Serwer musi posiadać deklarację CE lub równoważną.

## **Minimalne wymagane parametry - TYP 2:**

### **Obudowa:**

1. 2U
2. Obudowa serwerowa do montażu w szafie RACK 19" wraz z wysuwanymi szynami dedykowanymi do tego urządzenia przez producenta serwera.
3. Obudowa powinna posiadać wpanel LCD pozwalający jednoznacznie stwierdzić czy system działa poprawnie i pokazujący podstawowe stany działania serwera.
4. W obudowie powinien być zainstalowany zestaw redundantnych zasilaczy o mocy co najmniej 1100W w standardzie Titanium każdy wymienialnych podczas pracy oraz zestaw redundantnych wentylatorów.
5. Wentylatory powinny mieć możliwość wymiany podczas pracy systemu
6. Wbudowany czujnik otwarcia obudowy współpracujący z BIOS i kartą zarządzającą.
7. Obudowa powinna posiadać możliwość instalacji interfejsu NFC do połączenia z aplikacją zarządzającą serwerem na telefonie.
8. Aplikacja zarządzająca powinna być dostępna na Android i iOS

### **Płyta główna:**

9. Płyta główna obsługująca co najmniej dwa procesory i co najmniej
10. 16 slotów na pamięć taktowaną przynajmniej z częstotliwością 3200MT/s przy użyciu odpowiednich procesorów.
11. Płyta główna musi być zaprojektowana przez producenta serwera i oznaczona jego znakiem firmowym.
12. Musi być wyposażona w zaimplementowane sprzętowo mechanizmy kryptograficzne
13. Poświadczające integralność oprogramowania BIOS (Root of Trust),
14. Musi umożliwiać utworzenie bezpiecznego profilu w oparciu o konfigurację sprzętową oraz o
15. Konfigurację wewnętrznego oprogramowania komponentów serwera.
16. Zintegrowany z płytą główną moduł TPM w wersji co najmniej 2.0

### **Procesor:**

17. Dwa procesory typu skalowalnego z uwagi na licencjonowanie posiadające dokładnie po 8 rdzeni działające co najmniej z częstotliwością 2.8GHz i dające w teście Passmark dostępnym na stronie <https://www.cpubenchmark.net/> wynik nie mniejszy niż 19010

### **Pamięć RAM:**

18. 128GB pamięci RAM w modułach 32GB RDIMM przygotowanych na działanie z częstotliwością co najmniej 3200MT/s

### **Dyski:**

19. Miejsce na co najmniej 12 dysków w rozmiarze 3.5" wymienialne bez wyłączenia systemu.
20. Serwer ma mieć przewidzianą przez producenta możliwość dodania modułu pozwalającego na startowanie systemu z kart SD lub dysków M.2 skonfigurowanych w RAID1 nie zajmujących slotów na dyski.
21. Serwer powinien posiadać kontroler RAID umożliwiający konfigurację RAID 0, 1, 5, 10,50,6 posiadający co najmniej 8GB pamięci cache zabezpieczonej przed awarią prądu.
22. W serwerze powinny być zainstalowane co najmniej dwa dyski co najmniej 480GB SSD

**Dostawa sprzętu sieciowego i oprogramowania na potrzeby Gminy Cielądz  
w ramach programu "Cyberbezpieczny Samorząd"**

Or.SO.2714.13.2024

skonfigurowane fabrycznie w RAID 1 trzy dyski co najmniej 1.92GB SSD trzy dyski 8TB SAS

**Karta sieciowa:**

- 23. Na płycie głównej powinna być zainstalowana dwuportowa karta sieciowa 1GB BT
- 24. Karta nie może zajmować slotu PCIe
- 25. Oraz dwuportowa karta sieciowa 10GB BT
- 26. Karta nie może zajmować slotu PCIe

**Karta zarządzająca niezależna od zainstalowanego na serwerze systemu operacyjnego posiadająca dedykowane port RJ-45 Gigabit Ethernet umożliwiające:**

- 27. zdalny dostęp do graficznego interfejsu Web karty zarządzającej
- 28. szyfrowane połączenie (TLS) oraz autentykację i autoryzację użytkownika
- 29. możliwość podmontowania zdalnych wirtualnych napędów
- 30. wirtualną konsolę z dostępem do myszy, klawiatury
- 31. wsparcie dla IPv6 - wsparcie dla SNMP; IPMI2.0, VLAN tagging, SSH
- 32. możliwość zdalnego monitorowania w czasie rzeczywistym poboru prądu przez serwer, dane historyczne powinny być dostępne przez min. 7 dni wstecz.
- 33. możliwość zdalnego ustawienia limitu poboru prądu przez konkretny serwer
- 34. integracja z Active Directory
- 35. możliwość obsługi przez ośmiu administratorów jednocześnie
- 36. Wsparcie dla automatycznej rejestracji DNS - wsparcie dla LLDP
- 37. wysyłanie do administratora maila z powiadomieniem o awarii lub zmianie konfiguracji sprzętowej
- 38. możliwość podłączenia lokalnego poprzez złącze RS-232.
- 39. możliwość zarządzania bezpośredniego poprzez złącze microUSB umieszczone na froncie obudowy.
- 40. Monitorowanie zużycia dysków SSD
- 41. możliwość monitorowania z jednej konsoli min. 100 serwerami fizycznymi,
- 42. Automatyczne zgłaszanie alertów do centrum serwisowego producenta
- 43. Automatyczne update firmware dla wszystkich komponentów serwera
- 44. Możliwość przywrócenia poprzednich wersji firmware
- 45. Możliwość eksportu eksportu/importu konfiguracji (ustawienie karty zarządzającej, BIOSu, kart sieciowych, HBA oraz konfiguracji kontrolera RAID) serwera do pliku XML lub JSON
- 46. Możliwość zaimportowania ustawień, poprzez bezpośrednie podłączenie plików konfiguracyjnych
- 47. Automatyczne tworzenie kopii ustawień serwera w oparciu o harmonogram.

**Oprogramowanie zarządzające:****Dodatkowe oprogramowanie umożliwiające zarządzanie poprzez sieć, spełniające minimalne wymagania:**

- 48. wsparcie dla serwerów, urządzeń sieciowych oraz pamięci masowych;
- 49. możliwość zarządzania dostarczonymi serwerami bez udziału dedykowanego agenta;
- 50. wsparcie dla protokołów – WMI, SNMP, IPMI, WSMAN, Linux SSH;
- 51. możliwość oskryptowywania procesu wykrywania urządzeń;
- 52. możliwość uruchamiania procesu wykrywania urządzeń w oparciu o harmonogram;

**Dostawa sprzętu sieciowego i oprogramowania na potrzeby Gminy Cielądz  
w ramach programu “Cyberbezpieczny Samorząd”**

Or.SO.2714.13.2024

53. szczegółowy opis wykrytych systemów oraz ich komponentów;
54. możliwość eksportu raportu do CSV, HTML, XLS;
55. grupowanie urządzeń w oparciu o kryteria użytkownika;
56. automatyczne skrypty CLI umożliwiające dodawanie i edycję grup urządzeń;
57. szybki podgląd stanu środowiska;
58. podsumowanie stanu dla każdego urządzenia;
59. szczegółowy status urządzenia/elementu/komponentu;
60. generowanie alertów przy zmianie stanu urządzenia;
61. filtry raportów umożliwiające podgląd najważniejszych zdarzeń;
62. integracja z service desk producenta dostarczonej platformy sprzętowej;
63. możliwość przejęcia zdalnego pulpitu;
64. możliwość podmontowania wirtualnego napędu;
65. kreator umożliwiający dostosowanie akcji dla wybranych alertów;
66. możliwość importu plików MIB;
67. przesyłanie alertów „as-is” do innych konsol firm trzecich;
68. aktualizacja oparta o wybranie źródła bibliotek (lokalna, on-line producenta oferowanego rozwiązania);
69. możliwość instalacji sterowników i oprogramowania wewnętrznego bez potrzeby instalacji agenta;
70. możliwość automatycznego generowania i zgłaszania incydentów awarii bezpośrednio do centrum serwisowego producenta serwerów;
71. moduł raportujący pozwalający na wygenerowanie następujących informacji: nr seryjny sprzętu, konfiguracja poszczególnych urządzeń, wersje oprogramowania wewnętrznego, obsadzenie slotów PCIe i gniazd pamięci, informację o maszynach wirtualnych, aktualne informacje o stanie gwarancji, adresy IP kart sieciowych.

**Certyfikaty:**

72. Serwer musi być wyprodukowany zgodnie z normą ISO-9001:2015 lub równoważną oraz ISO-14001 lub równoważną
73. Serwer musi posiadać deklarację CE lub równoważną

**Warunki gwarancji:**

74. 2 lata gwarancji producenta, z czasem reakcji do następnego dnia roboczego od przyjęcia zgłoszenia - zgłoszenia przyjmowane 7 dni w tygodniu w trybie 24/7.
75. Gwarancja musi obejmować całość rozwiązania nie powinno być tak aby jakaś część tego rozwiązania nie podlegała gwarancji.
76. możliwość zgłaszania awarii poprzez ogólnopolską linię telefoniczną producenta.
77. Producent musi dawać możliwość rozszerzenia gwarancji do 7 lat
78. W przypadku naprawy dysku - uszkodzony dysk zostaje u klienta.
79. Podczas trwania gwarancji producent powinien zapewnić narzędzia i procesy do proaktywnej oceny stanu technicznego oraz automatycznego zgłaszania usterek bez ingerencji człowieka.
80. Powinna być możliwość skorzystania z pomocy wsparcia producenta za pomocą komunikatora np. messenger, teams, WhatsApp.
81. Firma serwisująca musi posiadać ISO 9001:2015 lub równoważne na świadczenie usług serwisowych oraz posiadać autoryzację producenta urządzeń.
82. Możliwość sprawdzenia statusu gwarancji poprzez stronę producenta podając unikatowy numer urządzenia oraz pobieranie uaktualnień mikrokodu oraz sterowników nawet w

- przypadku wygaśnięcia gwarancji serwera
83. Możliwość telefonicznego sprawdzenia konfiguracji sprzętowej serwera oraz warunków gwarancji po podaniu numeru seryjnego bezpośrednio u producenta lub jego przedstawiciela.

## VIII. AGREGAT PRĄDOTWÓRCZY

Niniejsza specyfikacja określa wymagania dotyczące zakupu i wdrożenia agregatu prądotwórczego. Celem jest zapewnienie niezawodnego i wydajnego źródła zasilania awaryjnego, które umożliwi podtrzymanie pracy kluczowych systemów i urządzeń w przypadku przerwy w dostawie energii elektrycznej. Agregat prądotwórczy ma zapewnić stabilne zasilanie w sytuacjach awaryjnych, umożliwiając nieprzerwaną pracę serwerowni, systemów komputerowych, instalacji telekomunikacyjnych, urządzeń medycznych oraz innych krytycznych elementów infrastruktury. Dodatkowo, agregat powinien oferować możliwość automatycznego przełączania zasilania w momencie wykrycia awarii, a także możliwość rozbudowy w celu dostosowania mocy do rosnących potrzeb zasilania. Agregat ma również posiadać funkcje monitorowania pracy, systemy zabezpieczające przed przeciążeniem oraz zapewniać łatwą obsługę serwisową.

Ilość: 1 szt.

### Minimalny zakres jaki musi spełniać dostarczony sprzęt/oprogramowanie:

1. Normy i standardy: 2006/42/CE, 2014/30/UE, 2014/35/UE, 2000/14/WE, 97/68/WE, EN 12100, EN 13857, EN 60204 lub równoważne
2. Wersja agregatu: Wersja obudowana, wyciszona, zgodna z IP według ISO 8528-13:2016 lub równoważne
3. Rok produkcji: Min. 2023
4. Producent: Jeden producent, urządzenie w całości przetestowane
5. Silnik i prądnica: Pochodzące z bieżącej produkcji
6. Konstrukcja: Wzmacniana, zabezpieczona przed odkształceniami, stal ocynkowana, malowanie klasa C4-H
7. Uchwyt załadunkowy: Centralny
8. Zawiasy: ze stali nierdzewnej, drzwi zamykane na klucz
9. Przycisk zatrzymania awaryjnego: Zewnętrzny
10. Amortyzatory drgań: Typu HD dla silnika i prądnicy
11. Osłony: Na elementy gorące i wirujące
12. Wymiary agregatu: 2300 x 1100 x 1500 mm (+/- 20 cm)
13. Ciężar własny (bez paliwa): 1000 kg (+/- 100 kg)
14. Wyciszenie: Wełna skalna, niepalna, atestowana
15. Poziom hałasu z 7m: Maksymalnie 65 dBA
16. Tłumik dźwięków: Stalowy, instalowany wewnątrz obudowy
17. Moc maksymalna: Min. 66 kVA (52 kW)
18. Moc znamionowa: 60 kVA (min. 48 kW)
19.  $\cos \varphi$ : 0,8
20. Napięcie: 400/230 V
21. Częstotliwość: 50 Hz
22. Silnik: Diesla, min. 4,5 litra, 4 cylindry, min. 88 hp
23. Pojemność zbiornika paliwa: Zapewniająca 24 godziny pracy przy 75% obciążenia

**Dostawa sprzętu sieciowego i oprogramowania na potrzeby Gminy Cielądz  
w ramach programu "Cyberbezpieczny Samorząd"**

Or.SO.2714.13.2024



24. Wlew paliwa: Na zewnątrz obudowy, zamykany na klucz
25. Filtr powietrza: Suchy
26. Chłodzenie silnika: Wodą
27. Prędkość obrotowa: 1500 r.p.m.
28. Układ elektryczny: 12 V
29. Akumulator rozruchowy: Tak
30. Ładowarka akumulatora: Automatyczna
31. Podgrzewanie bloku silnika: Automatyczne, kontrolowane przez panel sterowania
32. Prądnica: Renomowany europejski producent, spełniająca normy CEI 2-3, IEC 34-1, EN 60034-1, VDE 0530, BS 4999-5000
33. Regulacja napięcia: Automatyczna, tolerancja +/- 1%
34. Złącze prądnicy: Elastyczny dysk
35. Klasa IP prądnicy: IP 23
36. Klasa izolacji prądnicy: H
37. Panel sterowania: Pełne menu w języku polskim, tryby automatyczny, manualny, test i off. Ekran LCD, diody sygnalizacyjne, programowalna logika PLC, obsługa układu SZR, możliwość montażu modułów komunikacyjnych.
38. Szafa elektryczna/automatyka: Na podzespołach renomowanych producentów, zgodna z normami i standardami
39. Moduły komunikacyjne: RS485, LAN, Modbus, TCP/IP, SNMP, Profibus, GPRS

## **IX. SYSTEM ZARZĄDZANIA INFRASTRUKTURĄ INFORMATYCZNĄ KLASY ITSM**

**Ilość:** licencja na 35 stanowisk komputerowych oraz 1 licencja dostępowa do konsoli zarządzającej

### **Wymagania ogólne dla systemu zarządzania:**

1. Oprogramowanie musi posiadać polski oraz angielski interfejs językowy.
2. Oprogramowanie musi posiadać architekturę trójwarstwową składającą się z Bazy Danych, Serwera Aplikacji, Agenta/Konsoli zarządzającej.
3. Oprogramowanie musi umożliwiać obsługę dedykowanych kluczy szyfrujących podczas komunikacji pomiędzy agentami, serwer aplikacji i konsolą zarządzającą.
4. Odczyt informacji dotyczących parametrów sprzętowych komputera musi odbywać się za pośrednictwem agenta systemu instalowanego na komputerach użytkowników.
5. Agent systemu nie może nasłuchiwać na żadnym porcie sieciowym po stronie stanowiska komputerowego użytkownika.
6. Oprogramowanie musi umożliwiać wybór instalacji agenta w trybie standardowym oraz bezpiecznym tj. braku wkompiowanych funkcji takich jak zdalne zarządzanie, transfer plików, zdalny pulpit.
7. Oprogramowanie musi posiadać procedurę uwierzytelnienia i autoryzacji kont operatorów w konsoli zarządzającej poprzez fizyczne zabezpieczenie sprzętowe (lokalne lub sieciowe) wraz z hasłem, który umożliwia jednoczesną pracę wielu administratorom. Logowanie użytkowników konsoli zarządzającej musi umożliwiać integrację z kontami Active Directory. Wymagane zabezpieczenie sprzętowe musi posiadać mechanizm szyfrowania danych AES w obrębie przechowywania danych wrażliwych.
8. Oprogramowanie musi posiadać dodatkową autoryzację użytkownika konsoli zarządzającej za pomocą usługi Google Authenticator oraz Microsoft Authenticator.

9. Oprogramowanie musi posiadać moduł zarządzania uprawnieniami do poszczególnych funkcjonalności systemu dla operatorów konsoli zarządzającej zgodny z modelem RBAC (Role Based Access Control).
10. Oprogramowanie musi umożliwiać nadawanie oraz odbieranie uprawnień w czasie rzeczywistym (brak konieczności przelogowania użytkownika konsoli systemu).
11. Oprogramowanie musi umożliwiać blokadę wybranych uprawnień konkretnego użytkownika niezależnie od uprawnień wynikających z przypisanych ról.
12. Oprogramowanie musi współpracować z serwerem MSSQL Server 2008R2-2019
13. Oprogramowanie, w zakresie wszystkich warstw, nie może wymagać do prawidłowej pracy komponentów Java.
14. Oprogramowanie serwera aplikacji musi posiadać funkcjonalność centralnego wysyłania wybranych powiadomień mailowych .
15. Oprogramowanie musi posiadać moduł zarządzania uprawnieniami do danych w zakresie wybranych jednostek organizacyjnych oraz typów zasobów poszczególnych użytkowników konsoli. Wszelkie raporty, zestawienia oraz funkcje obejmują wtedy tylko wynikowe obiekty.
16. Oprogramowanie musi być podpisane cyfrowo przez Producenta ważnym certyfikatem, z prawidłową ścieżką certyfikacji, w której główny urząd certyfikacji (Root CA) jest uczestnikiem programu certyfikatów głównych systemu Windows. Podpis cyfrowy dotyczy składników Producenta systemu w zakresie plików wykonywalnych (\*.exe), plików bibliotek współdzielonych (\*.dll), plików sterowników (\*.sys) oraz pakietów instalacyjnych oprogramowania (\*.msi).
17. Oprogramowanie agentów musi posiadać obsługę sesji terminalowych Windows.
18. Oprogramowanie musi zapewniać dowolną konfigurację pracy wszystkich agentów, jednostek organizacyjnych, pojedynczego agenta, poprzez dziedziczenie definiowanych przez administratora parametrów. Zmiany konfiguracji agentów następują w trybie natychmiastowym (online).
19. Oprogramowanie musi posiadać raport przedstawiający różnice w konfiguracji poszczególnych agentów w stosunku do konfiguracji globalnej.
20. Oprogramowanie musi posiadać mechanizm logowania zmian w konfiguracji agentów przez użytkowników konsoli (data, czas, login, poprzednia i nowa wartość).
21. Oprogramowanie musi posiadać mechanizm analizy czasu pracy komputera, informujący użytkownika (alert oraz wymuszone działanie – restart) o przekroczeniu zadanego czasu pracy bez restartu systemu operacyjnego.
22. Oprogramowanie musi zapewniać automatyczny import drzewiastej struktury organizacyjnej zamawiającego (bez ograniczeń ilości zagnieżdżeń z kontenera Active Directory/OpenLDAP), kont użytkowników i komputerów z zachowaniem ich oryginalnego położenia wg. OU.
23. Oprogramowanie musi zapewniać w obrębie synchronizacji z Active Directory/OpenLDAP tworzenie listy filtrów zawężających węzły danych wraz z możliwością wskazania docelowej gałęzi struktury organizacyjnej lub lokalizacyjnej Zamawiającego.
24. Oprogramowanie musi posiadać kreator powiązań (mapowanie atrybutów) dowolnych atrybutów obiektów z usługi katalogowej do wskazanych atrybutów zasobów systemowych.
25. Oprogramowanie musi umożliwiać współpracę z nieograniczoną ilością kontrolerów domen z zachowaniem podległej struktury drzewiastej.
26. Oprogramowanie musi umożliwiać automatyczny import informacji dotyczących przynależności użytkowników oraz stanowisk komputerowych do grup struktury katalogowej.

27. Oprogramowanie musi posiadać raport przedstawiający informacje nt. grup struktury katalogowej wraz przynależącymi do nich użytkownikami.
28. Oprogramowanie musi umożliwiać tworzenie dynamicznych grup stanowisk w oparciu o kreator zawierający filtry (AND, OR) w zakresie min. wersja OS, nazwa oraz wersja wybranej aplikacji, RAM, CPU, HDD, jednostka organizacyjna, jednostka lokalizacyjna, architektura (x32, x64), zainstalowane oprogramowanie, wersja oprogramowania, lista usług systemowych, producent oraz model komputera, poziom uprawnień użytkownika, zainstalowana usługa systemowa, ostatnie uruchomienie systemu, obecność pliku EXE na dysku, predefiniowane atrybuty komputera (np. dostawca, numer faktury, data zakupu).
29. Oprogramowanie musi umożliwiać prezentację widoku zarządzanych stanowisk komputerowych w postaci listy stanowisk, drzewiastej struktury wg jednostek organizacyjnych, jednostek lokalizacyjnych, struktury Active Directory, struktury sieciowej (pule IP) oraz grup dynamicznych.
30. Oprogramowanie musi umożliwiać dynamiczne zawężanie wyników wyszukiwania ww. widoków na podstawie prezentowanych w nich atrybutów.
31. Oprogramowanie musi umożliwiać graficzną prezentację aktualnego stanu aktywności agenta (online/offline) z dokładnością do 1 minuty.
32. Oprogramowanie musi umożliwiać zapisywanie w bazie danych informacji o uruchomieniu i wyłączeniu komputera oraz zalogowaniu i wylogowaniu użytkownika.

#### **Inwentaryzacja konfiguracji komputerów:**

33. Oprogramowanie musi umożliwiać wydruk kartoteki sprzętowej stanowiska komputerowego.
34. Oprogramowanie musi umożliwiać samodzielną edycję wyglądu kartoteki sprzętowej, protokołów przekazania oraz zwrotu zasobów za pomocą graficznego kreatora wyglądu.
35. Oprogramowanie musi umożliwiać zapisywanie edytowanych szablonów (min. kartoteka sprzętowa, protokoły przekazania/zwrotu zasobów) w kontekście zalogowanego operatora konsoli zarządzającej.
36. Oprogramowanie musi umożliwiać projektowanie, generowanie oraz wydruk etykiet inwentaryzacyjnych w zakresie: model, nr inwentaryzacyjny, data zakupu, jednostka, wraz z obsługą kodów kreskowych w standardzie EAN128 oraz PDF417
37. Oprogramowanie musi umożliwiać okresową automatyczną inwentaryzację parametrów sprzętowych stanowiska: HDD, RAM, CPU, karta sieciowa, system operacyjny, karta graficzna itp.
38. Oprogramowanie Agenta musi umożliwiać audyt off-line, poprzez uruchomienie skanera (z GUI) bez konieczności instalacji, oraz zapis wyników do pliku w postaci zaszyfrowanej.
39. Oprogramowanie musi umożliwiać analizę sprzętową:
  - płyty głównej w zakresie model, producent, nr. seryjny,
  - CPU w zakresie nazwy, modelu, producenta, częstotliwości,
  - HDD w zakresie numeru seryjnego dysku, numeru seryjnego partycji, rozmiaru pamięci,
  - RAM w zakresie wielkości pamięci,
  - karty sieciowej w zakresie model, adres IP, adres MAC,
  - karty graficznej w zakresie model.
40. Oprogramowanie musi umożliwiać odczyt informacji dotyczących systemu operacyjnego w zakresie nazwy, wersji, daty instalacji, zainstalowanych poprawek, dostępnych kluczy licencyjnych, produkt ID.
41. Oprogramowanie musi umożliwiać odczyt informacji sieciowych w zakresie adresu IO, adresu MAC, nazwy sieciowej.
42. Oprogramowanie musi umożliwiać odczyt informacji sprzętowych z BIOS w zakresie nazwy BIOS, daty, producenta.

43. Oprogramowanie musi umożliwiać przegląd historii zmian parametrów sprzętowych komputerowych.
44. Oprogramowanie musi umożliwiać globalny przegląd stanowisk komputerowych pod względem parametrów sprzętowo-systemowych.
45. Oprogramowanie musi zawierać raport stanowisk komputerowych posiadających co najmniej jedno konto z uprawnieniami administratora.
46. Oprogramowanie musi umożliwiać odczyt urządzeń podłączonych do stanowiska komputerowego przez interfejs USB, z możliwością odczytania nazwy urządzenia, producenta, modelu oraz numeru seryjnego (o ile urządzenie dostarcza ww. informacji)
47. Oprogramowanie musi umożliwiać globalną analizę urządzeń podłączonych do stanowisk komputerowych przez interfejs USB
48. Oprogramowanie musi umożliwiać integrację z zewnętrzną usługą Dell API w celu automatycznego odczytania informacji na temat okresu gwarancji stanowiska komputerowego na podstawie odczytanego przez agenta identyfikatora (ServiceTag)
49. Oprogramowanie musi umożliwiać okresowe próbkowanie obciążenia procesora oraz zajętości pamięci RAM z możliwością zapisu odczytanych wyników do bazy w celu późniejszej analizy (historia obciążenia komputera).

#### **Inwentaryzacja oprogramowania:**

50. Oprogramowanie musi umożliwiać automatyczną inwentaryzację zainstalowanego na komputerach oprogramowania.
51. Oprogramowanie musi umożliwiać globalny przegląd wszystkich programów zainstalowanych na komputerach.
52. Oprogramowanie musi umożliwiać tworzenie zestawień zainstalowanych typów programów (freeware, shareware itp.).
53. Oprogramowanie musi umożliwiać tworzenie wykazów z zainstalowanym, dowolnie wybranym programem.
54. Oprogramowanie musi umożliwiać tworzenie zestawień zainstalowanych systemów operacyjnych na komputerach.
55. Oprogramowanie musi umożliwiać tworzenie wykazów stanowisk z brakiem zainstalowanego, dowolnie wybranego, programu.
56. Oprogramowanie musi posiadać wbudowany mechanizm umożliwiający, poprzez GUI konsoli, zdalną grupową dezinstalację oprogramowania np. pakietów MS Office.
57. Oprogramowanie musi umożliwiać oznaczanie kolorem aplikacji zabronionych oraz zgodnych ze standardem wraz z możliwością raportowania wg w/w klasyfikacji.
58. Oprogramowanie musi umożliwiać zablokowanie na stacji roboczej wybranych procesów celem uniemożliwienia ich uruchomienia przez użytkownika.
59. Oprogramowanie musi posiadać globalne zestawienie pozwalające na zdalne usunięcie nielegalnych danych np. plików AVI, MP3, MP4 bez konieczności fizycznej obecności użytkownika przy stacji.

#### **Zarządzanie licencjami, audyt oprogramowania:**

60. Oprogramowanie musi posiadać wbudowaną bazę sygnatur aplikacji (produktów) wraz z możliwością automatycznej aktualizacji wzorców ze strony Producenta oprogramowania
61. Oprogramowanie musi umożliwiać zdefiniowanie własnych sygnatur aplikacji (produktów) wykorzystywanych w procesie automatycznego audytu licencji (rozliczenie ilościowe).
62. Oprogramowanie musi umożliwiać wykonanie audytu licencji tj. systemowego porównania zidentyfikowanego na stanowiskach komputerowych oprogramowania (produktów) z zakupionymi licencjami wprowadzonymi do systemu jako odpowiednie



obiekty. Mechanizm audytu musi umożliwiać rozliczenie licencji z wykorzystaniem mechanizmów downgrade, upgrade.

- 63. Oprogramowanie musi umożliwiać zapis historii wykonywanych audytów licencji.
- 64. Oprogramowanie musi umożliwiać tworzenie bazy licencji systemowo/programowych i przypisywanie ich do stanowisk komputerowych oraz użytkowników.

#### **CMDB:**

- 65. Oprogramowanie musi umożliwiać tworzenie własnych typów elementów konfiguracji (CI)
- 66. Oprogramowanie musi umożliwiać dodawanie dowolnych atrybutów dla typów CI w szczególności: wartości logiczne, data/czas, numeryczne, tekstowe, słownikowe
- 67. Oprogramowanie musi umożliwiać tworzenie podrzędnych i nadrzędnych typów CI
- 68. Oprogramowanie musi umożliwiać dziedziczenie atrybutów przez elementy konfiguracji posiadające typ nadrzędny
- 69. Oprogramowanie musi umożliwiać tworzenie dowolnych typów relacji do obsługi połączeń pomiędzy różnymi typami CI
- 70. Oprogramowanie musi umożliwiać tworzenie atrybutów dla relacji
- 71. Oprogramowanie musi umożliwiać prezentowanie powiązań pomiędzy elementami konfiguracji w formie struktury płaskiej oraz graficznej
- 72. Oprogramowanie musi umożliwiać zbiorczy podgląd relacji pomiędzy poszczególnymi elementami konfiguracji
- 73. Oprogramowanie musi umożliwiać modelowanie struktury relacji pomiędzy usługami, sprzętem, organizacją oraz pracownikami
- 74. Oprogramowanie musi umożliwiać nadzór nad wpływem zmian na poszczególne elementy konfiguracji
- 75. Oprogramowanie musi umożliwiać import elementów konfiguracji ze źródeł takich jak usługa katalogowa, skaner sieci, zewnętrzne pliki płaskie (CSV)
- 76. Oprogramowanie musi umożliwiać tworzenie oraz edycję własnych list elementów konfiguracji
- 77. Oprogramowanie musi umożliwiać wyszukiwanie i analizę elementów konfiguracji wg posiadanych atrybutów
- 78. Oprogramowanie musi umożliwiać tworzenie własnych typów relacji z określaniem nazwy relacji podstawowe i odwrotnej
- 79. Oprogramowanie musi umożliwiać tworzenie własnych formularzy dla wszystkich elementów konfiguracji

#### **Zarządzanie zasobami oraz użytkownikami:**

- 80. Oprogramowanie musi umożliwiać tworzenie własnych szablonów widoków zasobów z określeniem analizowanych typów zasobów, widocznych atrybutów oraz informacji nt. powiązań pomiędzy zasobami.
- 81. Oprogramowanie musi umożliwiać tworzenie własnych atrybutów o typach co najmniej: tekst, liczba, bit, data, wartość słownikowa dla wybranego typu zasobu.
- 82. Oprogramowanie musi umożliwiać zapis oraz przegląd historii zmian dowolnego atrybutu zasobu w zakresie: operator, data, czas, poprzednia oraz nowa wartość.
- 83. Oprogramowanie musi umożliwiać zdefiniowanie dowolnych relacji pomiędzy zasobami (np. powiązania stanowiska z pracownikiem, licencją, innym zasobem) wraz z zapisem historii relacji zasobów.
- 84. Oprogramowanie musi umożliwiać przypisywanie do każdego z zarządzanych w systemie zasobów dokumentów typu: faktura zakupu, gwarancja, umowa serwisowa. Bazą



- dokumentów musi być centralne repozytorium umożliwiające powiązania dokumentów z zasobami w relacji 1:N wraz z podglądem przypisanych zasobów oraz wydrukiem.
85. Oprogramowanie musi umożliwiać zdefiniowanie dowolnego zasobu inwentaryzacyjnego (np. telefon, drukarka, nawigacja) w strukturze drzewiastej wraz z kreatorem widocznych/wymaganych atrybutów edycyjnych.
  86. Oprogramowanie musi posiadać dedykowaną (zintegrowaną z systemem) aplikację na platformę Android umożliwiającą spis z natury zinwentaryzowanych zasobów.
  87. Oprogramowanie musi umożliwiać import danych z zewnętrznego pliku CSV zawierającego informacje inwentaryzacyjne z nowo zakupionych urządzeń w zakresie: numer faktury, numer seryjny, model, nazwa, data zakupu.
  88. Oprogramowanie musi umożliwiać zaprojektowanie własnego schematu importu danych z zewnętrznego pliku CSV.
  89. Oprogramowanie musi umożliwiać automatyczne tworzenie relacji pracownik-komputer na podstawie atrybutów obiektu w usłudze katalogowej.
  90. Oprogramowanie musi zawierać wbudowany kreator wydruków w zakresie protokołów przekazania, zwrotu, likwidacji wraz z możliwością utworzenia dowolnego typu dokumentu
  91. Oprogramowanie musi umożliwiać export ww. protokołów w formacie PDF
  92. Oprogramowanie musi umożliwiać obsługę kodów kreskowych oraz QR w obrębie ww. kreatora wydruków
  93. Oprogramowanie musi umożliwiać użycie w kreatorze wydruków własnego logotypu organizacji
  94. Oprogramowanie musi umożliwiać użycie w kreatorze wydruków dowolnego atrybutu zasobu
  95. Oprogramowanie musi umożliwiać przypisanie dowolnej firmy serwisowej z bazy organizacji do zasobu
  96. Oprogramowanie musi umożliwiać przypisanie załącznika do zasobu
  97. Oprogramowanie musi umożliwiać pogląd wszystkich zgłoszeń serwisowych dotyczących danego zasobu
  98. Oprogramowanie musi umożliwiać podgląd zasobów (przypisanych do danego pracownika) z poziomu jego portalu użytkownika końcowego
  99. Oprogramowanie musi umożliwiać zarządzanie cyklem życia zasobu
  100. Oprogramowanie musi umożliwiać tworzenie niestandardowych reguł biznesowych dla zarządzania zasobami
  101. Oprogramowanie musi umożliwiać seryjne dodawanie zasobów
  102. Oprogramowanie musi umożliwiać automatyczne nadawanie numerów inwentaryzacyjnych dla zasobów
  103. Oprogramowanie musi udostępniać kreator raportów dla zasobów
  104. Oprogramowanie musi udostępniać możliwość kopiowania widoku dla określonego typu(ów) zasobu z innego typ zasobu
  105. Oprogramowanie musi udostępniać możliwość kopiowania formularz dla określonego typu(ów) zasobu z innego typ zasobu
  106. Oprogramowanie musi umożliwiać ewidencję magazynów
  107. Oprogramowanie musi umożliwiać ewidencję lokalizacji magazynowych
  108. Oprogramowanie musi umożliwiać ewidencję produktów magazynowych
  109. Oprogramowanie musi udostępniać informację o stanie magazynowym(ilościowo)
  110. Oprogramowanie musi umożliwiać generowanie dokumentów PZ/PW/RW/MM
  111. Oprogramowanie musi umożliwiać przyjęcie zasobów ewidencjonowanych i eksploatacyjnych na magazyn

- 112. Oprogramowanie musi umożliwiać wydawanie zasobów ewidencjonowanych i eksploatacyjnych z magazynu
- 113. Oprogramowanie musi umożliwiać zwrot zasobów na magazyn
- 114. Oprogramowanie musi umożliwiać zmianę szablonów dokumentów PZ/PW/RW/MM
- 115. Oprogramowanie musi umożliwiać wyszukiwanie dokumentów po dowolnym atrybucie
- 116. Oprogramowanie musi umożliwiać zarządzanie organizacjami/typami organizacji (np. klient, podwykonawca)
- 117. Oprogramowanie musi umożliwiać dowolne przypisanie osoby do organizacji
- 118. Oprogramowanie musi umożliwiać tworzenia dynamicznych grup użytkowników
- 119. Oprogramowanie musi umożliwiać zarządzanie kontaktami osób/organizacji
- 120. Oprogramowanie musi umożliwiać zarządzanie nieobecnościami użytkowników
- 121. Oprogramowanie musi umożliwiać zarządzanie uprawnieniami i poziomami dostępu do danych w zakresie zarządzania zasobami
- 122. Oprogramowanie musi umożliwiać automatyczne pobieranie danych rejestrowych kontrahentów z bazy GUS

### **Zdalny pulpit, zdalne zarządzanie komputerem:**

- 123. Oprogramowanie musi umożliwiać interakcję administratora z użytkownikiem, polegającą na podłączeniu do stanowiska (przejęcie pulpitu) administratora bez konieczności uprzedniego wylogowania użytkownika. Funkcjonalność zdalnego pulpitu nie może wymagać instalacji aplikacji firm trzecich, wymagane jest obsłużenie przejęcia zdalnego pulpitu przez mechanizm wbudowany w agencie (ten sam proces systemowy).
- 124. Oprogramowanie musi umożliwiać wybór monitora, którego ekran ma zostać przejęty podczas połączenia zdalnego. Podczas aktywnego połączenia zdalnego, użytkownik jest informowany o trwaniu sesji zdalnej poprzez wyświetlanie na aktywnym monitorze kontrastowego obramowania ekranu.
- 125. Oprogramowanie musi umożliwiać zdalne zarządzanie (bez użycia RDP/VNC itp.) lokalnymi kontami użytkowników w zakresie (tworzenie, usuwanie, edycja, zmiana hasła oraz typ konta).
- 126. Oprogramowanie musi umożliwiać wysyłanie polecenia Wake-on LAN.
- 127. Oprogramowanie musi umożliwiać zdalną dwukierunkową linię poleceń.
- 128. Oprogramowanie musi umożliwiać przesyłanie plików/katalogów od zdalnego użytkownika do administratora i/lub od administratora do zdalnego użytkownika bez względu na lokalizację sieciową komputera (LAN, WAN, Internet).
- 129. Oprogramowanie musi umożliwiać konfigurację przez administratora parametrów połączenia z użytkownikiem w zakresie: ilość kolorów, ilość klatek/sekundę, skalowanie okna użytkownika, jeżeli jest ono większe niż rozdzielczość stacji administratora.
- 130. Oprogramowanie musi umożliwiać wybór aktywnych sesji terminalowych, do których chcemy się podłączyć.
- 131. Oprogramowanie musi umożliwiać zbiorczy podgląd zdalnych pulpitów stacji.
- 132. Oprogramowanie musi posiadać zarządzanie technologią iAMT, vPro w zakresie uwzględniającym min.: Serial Over Lan (SOL), IDE Redirection (IDER), Hardware KVM, Assets.
- 133. Oprogramowanie musi zapewniać zdalną konfigurację technologii iAMT w trybie Client Control Configuration Mode.
- 134. Oprogramowanie musi umożliwiać zarządzanie stacjami komputerowymi poza siecią LAN/WAN, wymagane jest tylko dowolne połączenie internetowe
- 135. Oprogramowanie musi umożliwiać zdalne wykonywanie zapytań WQL
- 136. Oprogramowanie musi umożliwiać zdalny odczyt oraz modyfikację rejestru Windows

137. Oprogramowanie musi umożliwiać pełne wykorzystanie funkcji zawartych w sekcji zdalne zarządzanie dla stacji posiadających dowolne połączenie do sieci INTERNET bez konieczności zestawiania połączenia VPN
138. Oprogramowanie musi umożliwiać przejęcie pulpitu zdalnego z poziomu konsoli zarządzającej znajdującej się poza siecią LAN organizacji poprzez połączenie konsoli ze wskazanym serwerem aplikacji.
139. Oprogramowanie musi umożliwiać prowadzenie w czasie rzeczywistym dwukierunkowej komunikacji tekstowej (chat) pomiędzy użytkownikiem a administratorem.

### **Automatyzacja:**

140. Oprogramowanie musi umożliwiać zdalną instalację pakietów \*.msi, plików \*.cmd, \*.bat, \*.reg, \*.ps1 poprzez utworzenie zadań dystrybucji aplikacji oraz wskazanie docelowych komputerów lub grup komputerów za pomocą dedykowanego GUI użytkownika. Zadanie dystrybucji musi umożliwiać określenie okresu aktywności, godziny rozpoczęcia oraz przedstawiać status instalacji na wybranych stanowiskach.
141. Oprogramowanie musi umożliwiać tworzenie zadań dystrybucji polegające na jednorazowym uruchomieniu wybranego szablonu akcji na wybranych stanowiskach komputerowych.
142. Oprogramowanie musi umożliwiać tworzenie polis uruchamianych cyklicznie na wybranych stanowiskach komputerowych wg aktualnej przynależności do struktury organizacyjnej, lokalizacyjnej lub wybranych grup dynamicznych.
143. Oprogramowanie musi umożliwiać tworzenie dystrybucji zadań oraz polis dla wybranych stanowisk komputerowych poprzez interaktywny kreator (krok po kroku). Wybór odbiorców musi uwzględniać listę stanowisk, strukturę organizacyjną, strukturę lokalizacyjną oraz dynamiczne grupy stanowisk.
144. Oprogramowanie musi umożliwiać globalną dystrybucję plików oraz folderów do wskazanych lokalizacji do wybranych stanowisk komputerowych wg przynależności do struktury organizacyjnej, lokalizacyjnej lub grupy dynamicznej wraz z automatycznym (polisa) odtworzeniem brakujących danych w przypadku wykrycia niespójności.
145. Oprogramowanie musi umożliwiać szyfrowanie plików źródłowych dla zadań instalacji.
146. Oprogramowanie musi umożliwiać globalny przegląd postępu wykonania wybranych zadań oraz polis wraz z odczytem standardowego wyjścia (stdout) oraz standardowego wyjścia błędów (stderr).
147. Oprogramowanie musi umożliwiać tworzenie własnych szablonów akcji zawierających zdefiniowaną listę akcji pozwalających na warunkowe uruchamianie akcji zależnych (oczekiwanie na zakończenie akcji, praca w tle).
148. Oprogramowanie musi umożliwiać konfigurację typów akcji co najmniej w zakresie: dystrybucja i uruchomienie plików wsadowego BAT, dystrybucja plików rejestru REG, dystrybucja i instalacja pakietu MSI, dystrybucja i instalacja poprawki MSP, dystrybucja i uruchomienie aplikacji EXE, dystrybucja i uruchomienie skryptu PowerShell, dystrybucja plików i folderów, uruchomienie/wyłączenie/restart usługi systemowej, zakończenie procesu systemowego, wywołanie polecenia CMD.
149. Oprogramowanie musi umożliwiać konfigurowanie dedykowanych parametrów dla każdej z ww. akcji.
150. Oprogramowanie musi umożliwiać uruchomienie na prawach administracyjnych pliku instalacyjnego EXE (z GUI) w sesji użytkownika z ograniczonymi uprawnieniami do instalacji aplikacji. Proces instalacji jest manualnie kontynuowany przez użytkownika.
151. Oprogramowanie musi umożliwiać ograniczenie zakresu działania zadania, polisy oraz zawężenie wszelkich raportów systemowych do stanowisk spełniających kryteria wybranej dynamicznej grupy stanowisk.

152. Oprogramowanie w zakresie automatyzacji musi realizować m.in. następujące przypadki użycia z wykorzystaniem mechanizmu grup dynamicznych dla zadań oraz polis:
- Automatyczną instalacji aplikacji na komputerach spełniających warunki: stanowiska z Windows 10 z pamięcią RAM > 4GB i zainstalowaną wybraną aplikacją w wersji mniejszej (np. 7.0)
  - Automatyczne odinstalowanie aplikacji na komputerach spełniających warunki: stanowiska z Windows 7 gdzie producentem komputera jest np. Dell i zainstalowaną wybraną aplikacją w wersji większej niż (np. 8.0)
  - Dystrybucję plików oraz folderów (ze wskazaną zawartością np. dokumenty, skróty do aplikacji) na pulpity stanowisk komputerowych spełniających warunki: stanowiska z Windows 10 z brakiem zainstalowanej wybranej aplikacji oraz nie posiadające konta użytkownika z prawami administracyjnymi
  - Uruchomienia wybranego skryptu PowerShell dla komputerów spełniających warunki: stanowiska z Windows 10 w architekturze 32 bitowej, zainstalowaną aplikacją X w wersji większej niż (np. 6.0) i brakiem zainstalowanej aplikacji Y.
  - Uruchomienia wybranych szablonów akcji w przypadku wykrycia zmiany jednostki organizacyjnej stanowiska komputerowego.
153. W przypadku wcześniej zdefiniowanych polis wymagane jest, aby zostały one automatycznie uruchomione dla nowych stanowisk komputerowych po spełnieniu warunków przynależności do określonych grup dynamicznych.
154. Oprogramowanie musi umożliwić instalację oprogramowania z plików exe, które nie posiadają instalacji w trybie cichym poprzez automatyzację procesu manualnej instalacji (nagrywanie makr w zakresie wyborów typu zaznaczenie checkbox, wybór pozycji z listy, kliknięcie przycisku, wpisanie parametru/ścieżki itp.)
155. Oprogramowanie musi posiadać repozytorium szablonów makr automatyzacji do późniejszego wykorzystania podczas procesów instalacji
156. Oprogramowanie musi zawierać funkcję testowania nagranych makr z poziomu interfejsu użytkownika
157. Oprogramowanie musi wznawiać instalację, w przypadku przerwania procesu instalacji (np. z powodu wyłączenia komputera)
158. Nagrywanie makr musi być realizowane przez wybranie/wskazanie elementu okna, na którym ma zostać wykonana akcja (np. kliknięcie, wprowadzenie tekstu, zaznaczenie)
159. Oprogramowanie musi umożliwiać wysyłanie komunikatów (Windows Notification) do wskazanych stanowisk komputerowych (wybór manualny, wg struktury organizacyjnej, lokalizacyjnej lub grupy dynamicznej)
160. Oprogramowanie musi umożliwiać wysyłanie komunikatów przed każdą zdefiniowaną akcją automatyzacji (np.: przed rozpoczęciem instalacji pakietu MSI, przed dystrybucją plików, przed uruchomieniem skryptu PowerShell)
161. Oprogramowanie musi umożliwiać automatyzację procesu konfiguracji dowolnej aplikacji Windows w celu odtworzenia zapamiętanych akcji (makr) dla wskazanych stanowisk komputerowych.

### **Backup danych użytkownika:**

162. Oprogramowanie musi umożliwiać tworzenie dowolnej ilości automatycznych zadań w zakresie archiwizacji danych – globalnie z poziomu głównej konsoli zarządzającej.
163. Oprogramowanie musi umożliwiać globalną zmianę parametrów zadań archiwizacji (ilość archiwów, kompresja, okres, zakres).



164. Oprogramowanie musi umożliwiać definiowanie rozszerzeń plików, które mają być pomijane podczas procesu archiwizacji oraz rozszerzeń plików np. \*.doc, które mają być archiwizowane.
165. Oprogramowanie Agenta musi umożliwiać kopię całościową danych oraz przesyłanie plików z archiwizacji na wskazany serwer FTP.
166. Mechanizm archiwizacji danych musi być realizowany przez Agenta systemu bez udziału zdalnych sesji (typu zdalny pulpit, wywoływanie skryptów)
167. Oprogramowanie musi umożliwiać definiowanie cyklu archiwizacji.
168. Oprogramowanie musi umożliwiać automatyczne usuwanie starszych plików kopii całościowej, definiowanie globalnego zadania archiwizacji.
169. Zarządzanie urządzeniami USB Storage
170. Oprogramowanie musi umożliwiać zapisywanie w bazie danych informacji o kopiowaniu z/do urządzeń zewnętrznych typu: Pendrive USB, dysk zewnętrzny.
171. Oprogramowanie musi posiadać raport w zakresie rejestracji informacji na temat użytkownika, który kopiował i/lub uruchamiał napęd, kiedy miało miejsce zdarzenie i jakie dokumenty zostały skopiowane.
172. Oprogramowanie musi umożliwiać blokadę oraz autoryzację wybranych urządzeń USB w obrębie klasy USBStorage.
173. Oprogramowanie musi umożliwiać włączenie trybu ReadOnly dla klasy USBStorage
174. Oprogramowanie musi umożliwiać całkowitą blokadę klasy FDD/CD/DVD

#### **Monitoring stanowisk komputerowych:**

175. Oprogramowanie musi umożliwiać zestawienie najpopularniejszych adresów (jakie stanowiska je wywoływały, kiedy) z możliwością zapisu całego adresu lub tylko głównej strony.
176. Oprogramowanie umożliwia zestawienie najaktywniejszych stanowisk (pod kątem WWW), jakie adresy odwiedzały, kiedy, wszystkie zestawienia do poziomu: jednostka organizacyjna, stanowisko, zalogowany użytkownik.
177. Oprogramowanie musi umożliwiać analizę uruchamianych aplikacji (aktywność stanowisk wg aplikacji oraz wykorzystanie zainstalowanych aplikacji wg stanowisk).
178. Oprogramowanie musi umożliwiać analizę efektywności pracy użytkowników na poszczególnych aplikacjach
179. Oprogramowanie musi umożliwiać blokadę stron www (biała i czarna lista adresów, blokada pełna lub selektywna) z możliwością automatycznego zamykania przeglądarki lub konkretnej karty przeglądarki (w przypadku wykrycia adresu zabronionego).
180. Oprogramowanie musi umożliwiać tworzenie statystyk aktywności stron WWW oraz aktywności stanowisk.
181. Oprogramowanie musi umożliwiać podział stron na dozwolone i zabronione.
182. Oprogramowanie musi umożliwiać wydruki tabelaryczne oraz graficzne (wykresy aktywności).
183. Oprogramowanie musi umożliwiać okresowe tworzenie zrzutu ekranu użytkownika z możliwością przesłania go na serwer.
184. Oprogramowanie musi umożliwiać rozróżnienie stanów monitorowanego komputera w szczególności stan aktywności (focus okna), hibernacji, uśpienia oraz wylogowania
185. Oprogramowanie musi umożliwiać odczyt aktywności użytkownika w czasie rzeczywistym w zakresie min. tytuł okna, adres www przeglądanej strony z dokładnością do 1 sekundy.
186. Oprogramowanie musi umożliwiać analizę aktywności myszy oraz klawiatury dla poszczególnych monitorowanych aplikacji oraz stron internetowych (ilość kliknięć).



187. Oprogramowanie musi umożliwiać monitorowanie wszystkich prac drukowania generowanych na urządzeniach sieciowych udostępnionych przez centralny serwer wydruków i udostępnionych lokalnie przez port TCP/IP
188. Oprogramowanie musi umożliwiać monitorowanie wszystkich prac drukowania generowanych na urządzeniach lokalnych udostępnionych przez port LPT, USB. Monitorowanie tych wydruków musi odbywać się poprzez agenta aplikacji zainstalowanego na stacji roboczej będącej serwerem wydruków dla drukarki lokalnej.
189. Oprogramowanie po zainstalowaniu musi przysyłać do serwera aplikacji następujące informacje: nazwa stacji roboczej, nazwa zainstalowanego sterownika drukarki, nazwa portu z jakiego dany sterownik korzysta, opis sterownika drukarki, format drukowanych stron oraz nazwę drukowanego dokumentu.
190. Oprogramowanie musi posiadać możliwość definicji kosztów wydruku dla poszczególnych urządzeń drukujących (podział kosztu na mono/kolor).

### **ServiceDesk – Zarządzanie zgłoszeniami:**

191. Oprogramowanie w części HelpDesk musi być oparte na zasadach ITIL w szczególności:
  - Zarządzanie problemem
  - Zarządzanie incydem
  - Obsługa procesów poprzez WorkFlow (wnioski o usługi, uprawnienia, zakupy)
  - Zarządzanie umowami serwisowymi
  - Definicje poziomów SLA (reakcja, naprawa, reklamacja)
192. Oprogramowanie musi umożliwiać zgłaszania przez użytkowników z poziomu przeglądarki WWW (dedykowany portal) awarii sprzętu, usług, oprogramowania i innych typów awarii zdefiniowanych przez administratora.
193. Portal ServiceDesk musi mieć możliwość obsługi przez wiodące przeglądarki WWW na urządzeniach mobilnych poprzez responsywny interfejs użytkownika.
194. Portal ServiceDesk musi umożliwiać wybór wersji językowej interfejsu (co najmniej polski i angielski).
195. Obsługa listy zgłoszeń serwisowych (incydentów i problemów) musi być realizowana przez portal ServiceDesk z zachowaniem nadanego poziomu uprawnień.
196. Oprogramowanie musi umożliwiać kontrolę obciążenia działu IT, optymalizację podziału pracy pomiędzy pracowników działu IT oraz przegląd awaryjności sprzętu.
197. Oprogramowanie musi umożliwiać uwierzytelnianie użytkowników wykorzystując bazę Active Directory poprzez protokół LDAP.
198. Oprogramowanie musi umożliwiać automatyczne autoryzowanie określonych stanowisk i użytkowników (z wykorzystaniem mechanizmu SSO), aby uniknąć każdorazowego uwierzytelniania przed korzystaniem z systemu zgłoszeń.
199. Oprogramowanie musi umożliwiać sortowanie listy zgłoszeń awarii, wg daty zgłoszenia, priorytetu, statusu.
200. Oprogramowanie musi umożliwiać filtrację zgłoszeń wg priorytetu oraz statusów zgłoszeń, stanowisk oraz inżynierów obsługujących zgłoszenia.
201. Oprogramowanie musi umożliwiać tworzenie dedykowanych list zgłoszeń z różnymi danymi, domyślnym filtrowaniem i sortowaniem.
202. Oprogramowanie musi umożliwiać określenie widoczności poszczególnych list zgłoszeń w zależności od zalogowanego użytkownika.
203. Oprogramowanie musi umożliwiać określenie widoczności zgłoszeń w zależności od kategorii i lokalizacji zgłoszeń przypisanych do zalogowanego użytkownika.
204. Oprogramowanie musi umożliwiać dostęp do zgłoszeń swoich podwładnych przez przełożonego.

205. Oprogramowanie musi umożliwiać dodawanie przez administratora nowych wpisów (komentarzy) w zgłoszeniu, jak i umożliwiać zmianę statusu sprawy. Użytkownik także ma możliwość dodawania nowych wpisów do zgłoszonego problemu wraz ze zmianą statusu.
206. Oprogramowanie musi umożliwiać tworzenie zadań w ramach konkretnego zgłoszenia z możliwością przekazania do realizacji przez innych użytkowników.
207. Oprogramowanie musi umożliwiać tworzenie globalnych zadań do realizacji przez zalogowanego użytkownika.
208. Oprogramowanie musi umożliwiać tworzenie szablonów zadań.
209. Oprogramowanie musi umożliwiać rejestrację czasu pracy poświęconego na realizację zgłoszenia przez opiekuna.
210. Oprogramowanie musi umożliwiać przysyłanie użytkownikom powiadomień pocztą elektroniczną o nowych wpisach i zmianach w zgłoszeniu.
211. Oprogramowanie musi umożliwiać edycję szablonów powiadomień email.
212. Oprogramowanie musi umożliwiać tworzenie wielopoziomowych list kategorii zawierających nazwę i opis kategorii.
213. Oprogramowanie musi umożliwiać określenie widoczności poszczególnych kategorii w zależności od zalogowanego użytkownika.
214. Oprogramowanie musi umożliwiać tworzenie pól dodatkowych na formularzu rejestracji zgłoszenia.
215. Oprogramowanie musi umożliwiać określenie widoczności poszczególnych pól dodatkowych w zależności od zalogowanego użytkownika.
216. Rozwiązania w bazie wiedzy muszą posiadać znacznik określający czy są dostępne dla użytkowników, czy są wewnętrznymi uwagami działu IT. Panel www użytkownika musi zawierać wyszukiwarkę tematów wg słów kluczowych oraz wewnętrznej treści.
217. Oprogramowanie musi umożliwiać edycję bazy wiedzy z poziomu przeglądarki WWW wraz z możliwością formatowania tekstu (wraz z grafiką) oraz wstawiania załączników.
218. Oprogramowanie musi umożliwiać administratorowi wprowadzenie do systemu zgłoszenia użytkownika, który nie ma dostępu do PC (np. telefoniczna informacja o awarii komputera).
219. Oprogramowanie musi umożliwiać delegowanie zgłoszenia innemu administratorowi (technikowi), jak również przejęcie innego zgłoszenia (np. w przypadku nieplanowanej nieobecności pracownika).
220. Oprogramowanie musi umożliwiać obsługę tzw. Linii wsparcia poprzez samodzielne tworzenie nowych linii wraz z przypisywaniem do nich dowolnej ilości kont operatorów HelpDesk. Zgłoszenie serwisowe musi mieć możliwość przekazania do dowolnej linii wsparcia lub dedykowanego operatora HelpDesk. Linia wsparcia musi mieć możliwość przypisania powiązanych z nią kategorii zgłoszeń.
221. Oprogramowanie musi umożliwiać informowanie pracowników o planowanych działaniach, awariach za pomocą komunikatów wprowadzanych na stronę główną panelu zgłaszania usterki, bądź do poszczególnych kategorii.
222. Oprogramowanie musi umożliwiać określenie widoczności komunikatów o planowanych działaniach, awariach w zależności od zalogowanego użytkownika.
223. Oprogramowanie musi umożliwiać tworzenia baz umów serwisowych powiązanych z bazami firm serwisowych (dostawców sprzętu, oprogramowania, lokalnych serwisów). lub z zakupionym sprzętem.
224. Oprogramowanie w oparciu o bazę firm/umów serwisowych musi umożliwiać zapis przekazania zgłoszenia do serwisu zewnętrznego.
225. Oprogramowanie musi umożliwiać przysyłanie powiadomień do firm serwisowych powiązanych ze zgłoszeniem.

226. Oprogramowanie musi posiadać możliwość rejestracji w historii zgłoszenia (w komentarzach) korespondencji.
227. mailowej między opiekunami zgłoszenia a firmami serwisowymi powiązanymi ze zgłoszeniem.
228. Oprogramowanie musi posiadać dedykowane panele WWW w zależności od aktywnie zalogowanego użytkownika końcowego (panel dla użytkownika tj. zgłaszanie incydentów, panel dla operatora serwisowego – obsługa zgłoszeń, panel dla managera HelpDesk – analiza graficzna oraz tabelaryczna pracy operatorów HelpDesk).
229. Oprogramowanie musi umożliwiać wyświetlenie w panelu WWW użytkownika informacji nt. powiązanych z użytkownikiem zasobów (przypisane stanowiska PC, przydzielone licencje aplikacji, wydane urządzenia).
230. Oprogramowanie musi umożliwiać wybranie zasobu w określonej kategorii powiązanego z użytkownikiem podczas rejestracji zgłoszenia.
231. Oprogramowanie musi umożliwiać tworzenie zgłoszeń cyklicznych z możliwością definiowania częstości występowania oraz typu okresu (codziennie, co tydzień, co miesiąc)
232. Oprogramowanie musi umożliwiać tworzenie reguł w celu automatyzacji obsługi zgłoszeń. Reguły muszą uruchamiać się w odpowiedzi na określone zdarzenia w systemie i wykonywać akcje w zależności od spełnionych warunków. W zakresie reguł ServiceDesk musi realizować m.in. następujące przypadki użycia:
- Zmiana statusu po przejściu zgłoszenia przez opiekuna.
  - Przejmowanie zadań po przejściu zgłoszenia przez opiekuna.
  - Dodawanie zadań w zgłoszeniu w zależności od parametrów zgłoszenia.
  - Wznawianie zgłoszenia po odpowiedzi przez zgłaszającego użytkownika.
  - Zamykanie zgłoszenia po upływie czasu bez odpowiedzi użytkownika.
  - Zamykanie zgłoszenia po upływie czasu reklamacji.
  - Dodawanie wpisów (komentarzy) w zgłoszeniu na podstawie szablonów.
  - Zmiana parametrów zgłoszenia po znalezieniu wybranej frazy w treści komentarza.
  - Walidacja zamkniętych zadań w zamykanym zgłoszeniu.
  - Systemowe potwierdzanie realizacji zgłoszenia.
  - Wysyłanie dodatkowych powiadomień cyklicznych ze zgłoszeniami, np. zgłoszenia wymagające reakcji, zgłoszenia do realizacji lub zgłoszenia wstrzymane/wznowione.
233. Oprogramowanie musi umożliwiać tworzenie szablonów komentarzy wykorzystywanych przez opiekunów zgłoszeń.
234. Oprogramowanie musi posiadać możliwość rejestracji zgłoszeń i komentarzy drogą mailową, zarówno przez zarejestrowanych użytkowników systemu jak i niezarejestrowanych użytkowników.
235. Oprogramowanie musi umożliwiać obsługę dowolnej ilości kont pocztowych do wysyłania powiadomień i generowania zgłoszeń/komentarzy przez email.
236. Oprogramowanie musi posiadać wbudowane raporty prezentujące m.in. realizację obsługi zgłoszeń w zakładanym SLA (statystyka miesięczna, kwartalna, roczna).
237. Oprogramowanie musi umożliwiać definiowanie własnych widoków oraz zestawień dla każdego zalogowanego użytkownika
238. Oprogramowanie musi umożliwiać zdefiniowanie własne macierzy priorytetów na podstawie pilności oraz wpływu zgłoszenia
239. Oprogramowanie musi umożliwiać zamodelowanie trzy zmianowego trybu pracy inżynierów (opiekunów zgłoszeń)
240. Oprogramowanie musi umożliwiać informowanie użytkowników o nowych zdarzeniach systemowych za pomocą notyfikacji (dymku) podczas pracy z systemem

- 241. Oprogramowanie musi umożliwiać tworzenie obiegu procesu decyzyjnego dla wniosków o uprawnienia lub elementy konfiguracji w oparciu o bazę CMDB
- 242. Oprogramowanie musi umożliwiać zaprojektowanie dowolnego formularza do wprowadzania danych z wykorzystaniem własnych atrybutów (wraz ze zmianą układu/położenia atrybutów w projektowanym widoku)
- 243. Oprogramowanie musi umożliwiać definicję czasów SLA w oparciu o matrycę priorytetów, statusy, kategorie lub dowolne warunki i atrybuty zgłoszenia
- 244. Oprogramowanie musi umożliwiać dodanie Akceptacji do już istniejącego zgłoszenia
- 245. Oprogramowanie musi umożliwiać definiowanie własnych reguł zarządzania w oparciu o warunki i akcje dla Prawdy i Fałszu (zdarzenie -> warunek -> akcja)
- 246. Oprogramowanie musi umożliwiać tworzenie wielu zgłoszeń poprzez wybór kilku użytkowników w zgłoszeniu
- 247. Oprogramowanie musi umożliwiać tworzenie słowników wartości dla atrybutów w oparciu o strukturę płaską lub drzewiastą
- 248. Oprogramowanie musi umożliwiać tworzenie atrybutów zależnych poprzez określone warunki widoczności
- 249. Oprogramowanie musi umożliwiać definiowanie formularzy zamykających zgłoszenie oraz zatwierdzające zmiany w zgłoszeniu
- 250. Oprogramowanie musi umożliwiać definiowanie reguł biznesowych za pomocą graficznego/blokowego kreatora.
- 251. Oprogramowanie musi umożliwiać definiowanie obiegu za pomocą graficznego/blokowego kreatora.
- 252. Oprogramowanie musi umożliwiać tworzenie niestandardowych raportów za pomocą kreatora.
- 253. Oprogramowanie musi umożliwiać definiowanie poziomu dostępu do zgłoszeń dla dynamicznych grup użytkowników.
- 254. Oprogramowanie musi umożliwiać definiowanie formularzy dla zgłoszeń w danej kategorii za pomocą kreatora Drag&Drop z możliwością określenia układu kolumn.
- 255. Oprogramowanie musi umożliwiać tworzenie dowolnej liczby Dashboard-ów dla użytkownika za pomocą kreatora Drag&Drop.
- 256. Oprogramowanie musi umożliwiać zmianę układu szczegółów zgłoszenia za pomocą kreatora Drag&Drop.
- 257. Oprogramowanie musi umożliwiać udostępniania ogłoszeń w formie Widget-u oraz okienka modalnego z wymaganym potwierdzeniem dla użytkownika.
- 258. Oprogramowanie musi umożliwiać zaprojektowanie dowolnego szablonu protokołu zgłoszenia.
- 259. Oprogramowanie musi udostępniać matrycę(wpływ/pilność) dla obliczania priorytetu zgłoszeń.
- 260. Oprogramowanie musi umożliwiać zmianę koloru dla statusu/priorytetu/wpływu/pilności zgłoszenia prezentowanego na liście zgłoszeń.
- 261. Oprogramowanie musi umożliwiać definiowanie dowolnych kolejek zgłoszeń.
- 262. Oprogramowanie musi umożliwiać rejestrację nieobecności administratorów z możliwością wybrania zastępstwa.

#### **ServiceDesk – Zarządzanie wnioskami:**

- 263. Oprogramowanie musi zapewnić obsługę Workflow w zgłoszeniach serwisowych poprzez zdefiniowanie logicznych ścieżek (zbiór węzłów logicznych).
- 264. Oprogramowanie musi umożliwiać wybór wielu zasobów na jednym formularzu wniosku. Przykładowo dla wniosku o nadanie uprawnień musi istnieć możliwość wskazania wielu systemów/zbiorów danych z podziałem na moduły lub poziomy uprawnień użytkownika.



265. Na poziomie każdego węzła logicznego w workflow musi być możliwość edycji/modyfikacji zawartości danych w szczególności statusu, uwag, załączników (o dowolnym typie pliku) wraz z utworzeniem wpisu w historii przetwarzanego obiegu.

#### **ServiceDesk – Zarządzanie uprawnieniami:**

- 266. Oprogramowanie musi umożliwiać inwentaryzację Systemów Informatycznych oraz Zbiorów danych
- 267. Oprogramowanie musi umożliwiać określanie powiązań pomiędzy pracownikami z Systemami Informatycznymi oraz Zbiorami danych
- 268. Oprogramowanie musi umożliwiać budowanie powiązanych zestawów atrybutów dla Systemów Informatycznych oraz Zbiorów danych (np. termin ważności dostępu, poziom dostępu, przetwarzanie danych wrażliwych)
- 269. Oprogramowanie musi umożliwiać tworzenie ścieżek decyzyjnych dla dowolnych wniosków o uprawnienia do Systemów Informatycznych oraz Zbiorów danych
- 270. Oprogramowanie musi umożliwiać akceptację poszczególnych etapów przez dedykowane osoby decyzyjne zdefiniowane w konfiguracji ścieżek
- 271. Oprogramowanie musi umożliwiać akceptację etapów ścieżki przez automatyczny wybór powiązanych opiekunów merytorycznych oraz technicznych
- 272. Oprogramowanie musi umożliwiać definiowanie dowolnych akcji dla poszczególnych kroków (np. zmiana opiekuna, statusu)
- 273. Oprogramowanie musi umożliwiać automatyczne tworzenie powiązań pracownika z Systemem informatycznym lub Zbiorem danych po akceptacji wniosku
- 274. Oprogramowanie musi umożliwiać obsługę procesu (wniosku) o odebranie uprawnień (koniec terminu dostępu, zwolnienie pracownika)
- 275. Oprogramowanie musi umożliwiać raportowanie uprawnień wg Systemów Informatycznych oraz Zbiorów danych dla poszczególnych osób
- 276. Oprogramowanie musi umożliwiać raportowanie uprawnień w pracowników do Systemów Informatycznych oraz Zbiorów danych
- 277. Oprogramowanie musi umożliwiać generowanie edytowalnej Karty Uprawnień Pracownika

#### **ServiceDesk – Zarządzanie rezerwacjami:**

- 278. Oprogramowanie musi umożliwiać rezerwację dowolnego aktywnego zasobu w systemie.
- 279. Oprogramowanie musi umożliwiać kategoryzowanie rejestrowanych rezerwacji.
- 280. Oprogramowanie musi umożliwiać określenie widoczności poszczególnych kategorii rezerwacji w zależności od zalogowanego użytkownika.
- 281. Oprogramowanie musi informować o możliwych konfliktach podczas tworzenia/edycji rezerwacji z zasobem.
- 282. Oprogramowanie musi prezentować informacje o rezerwacjach w formie graficznej – kalendarza.
- 283. Oprogramowanie musi umożliwiać akceptację, odrzucenie lub anulowanie rezerwacji przez upoważnionych użytkowników.

#### **Monitoring sieci LAN:**

- 284. Oprogramowanie musi umożliwiać okresowe skanowanie sieci LAN (wg. zadanych kryteriów, na wybranych serwerach lokalnych) z wykorzystaniem protokołu SNMP, celem prezentacji aktywnych urządzeń IP w zakresie co najmniej komputery, drukarki, routery, smartfony



- 285. Oprogramowanie musi umożliwiać monitorowanie poprzez wykorzystanie protokołu SNMP stanu drukarek tj. poziomy tonerów, liczba wydrukowanych stron oraz informować błędach takich jak brak papieru, zacięcie papieru.
- 286. Oprogramowanie musi umożliwiać wizualizację ruchu sieciowego na poszczególnych portach urządzeń sieciowych wraz z wizualizacją w postaci mapy sieci dla wskazanego urządzenia typu switch, router.
- 287. Oprogramowanie musi umożliwiać z zdalną instalację agenta systemu z poziomu wykrytej struktury sieciowej z wykorzystaniem poświadczeń administracyjnych, w tym również stanowisk poza usługą katalogową.
- 288. Oprogramowanie musi umożliwiać monitorowanie stanu dowolnej usługi sieciowej TCP.
- 289. Oprogramowanie musi umożliwiać monitorowanie dowolnego licznika SNMP(v1/2/3) urządzenia.
- 290. Oprogramowanie musi umożliwiać monitorowanie stanu dowolnego urządzenia sieciowego poprzez odpytywanie typu PING.
- 291. Oprogramowanie musi umożliwiać tworzenie konfigurowalnych zdarzeń sieciowych powodujących wysyłanie komunikatów informacyjnych i/lub ostrzegawczych poprzez SMS i/lub Email.

#### **Zarządzanie dokumentami:**

- 292. Oprogramowanie musi umożliwiać centralną ewidencję dokumentów
- 293. Oprogramowanie musi umożliwiać zawierać dedykowany formularz dodawania nowego dokumentu z możliwością edycji widocznych oraz wymaganych atrybutów dokumentu
- 294. Oprogramowanie musi umożliwiać dołączenie skanu dokumentu (m.in.: skany faktur, umów)
- 295. Oprogramowanie musi umożliwiać stworzenie dedykowanego zbioru ról i uprawnień w zakresie obsługi rejestru dokumentów
- 296. Oprogramowanie musi umożliwiać utworzenie pomocniczych rejestrów oraz słowników
- 297. Oprogramowanie musi umożliwiać przeszukiwanie bazy dokumentów oraz kontrahentów po dowolnie wskazanym atrybucie opisującym
- 298. Oprogramowanie musi umożliwiać utworzenie rejestru osób reprezentujących
- 299. Oprogramowanie musi umożliwiać analizę zmian wartości dowolnych atrybutów opisujących dokument w zakresie daty zmiany, aktualnej/poprzedniej wartości oraz osoby dokonującej zmiany

#### **System wewnętrznego komunikatora dla użytkowników**

- 300. Oprogramowanie musi zawierać wewnętrzny komunikator pracujący w sieci LAN, integrujący się z usługą katalogową w zakresie kont użytkowników (dane osobowe, avatar), jednostek organizacyjnych.
- 301. Oprogramowanie w zakresie modułu komunikatora dla użytkowników musi współpracować z serwerem MSSQL Server 2008R2-2019 lub PostgreSQL
- 302. Oprogramowanie komunikatora musi umożliwiać automatyczne logowanie użytkowników pochodzących z usługi katalogowej.
- 303. Oprogramowanie komunikatora musi umożliwiać konwersację grupową oraz prywatną pomiędzy użytkownikami
- 304. Oprogramowanie komunikatora musi umożliwiać wysyłanie wiadomości powitalnych; komunikatów grupowych z raportowaniem doręczenia oraz odczytania.
- 305. Oprogramowanie komunikatora musi umożliwiać generowanie raportów doręczenia/ odczytania wiadomości wymagających potwierdzenia.
- 306. Oprogramowanie komunikatora musi umożliwiać określenie maksymalnego rozmiaru transferowanego pliku (przez administratora).

- 307. Oprogramowanie komunikatora musi umożliwiać wysyłanie powiadomień e-mail o utworzeniu/modyfikacji użytkowników, którzy nie pochodzą z usługi katalogowej.
- 308. Oprogramowanie komunikatora musi umożliwiać automatyczną aktualizację wg. zadanej konfiguracji danych synchronizowanych (ze szczególnym uwzględnieniem danych o użytkownikach, jednostkach organizacyjnych z usługi katalogowej).
- 309. Oprogramowanie komunikatora musi umożliwiać archiwizację starych rozmów między użytkownikami.
- 310. Oprogramowanie komunikatora musi umożliwiać administratorowi wyłączenie globalnie możliwości zamknięcia/wylogowanie/zapisywanie poświadczeń dla klientów końcowych.
- 311. Oprogramowanie komunikatora musi umożliwiać administratorowi bezpieczeństwa wgląd do rozmów pracowników, wyłączenie wybranych funkcjonalności dla klienta końcowego (np. transferu plików, konferencji audio-video).
- 312. Oprogramowanie komunikatora musi umożliwiać wymianę plików pomiędzy zalogowanymi użytkownikami
- 313. Oprogramowanie komunikatora musi umożliwiać nawiązanie sesji audio oraz wideo pomiędzy zalogowanymi użytkownikami wraz z obsługą konferencji grupowych.

**Wymagania formalne:**

- 314. Dostarczone licencje na oprogramowanie muszą być bezterminowe.
- 315. Dostarczone licencje na oprogramowanie muszą być dostarczone z 12 miesięcznym supportem producenta, liczonym od daty zakończenia wdrożenia.
- 316. Obsługa serwisowa w zakresie obsługi błędów realizowana ma być z czasem reakcji 16 godzin roboczych oraz czasem naprawy 80 godzin roboczych. W ramach supportu wymagany jest dostęp do nowych wersji systemu oraz wsparcia technicznego producenta.
- 317. Dostarczone licencje na oprogramowanie muszą objąć co najmniej 35 stanowisk komputerowych z systemem klasy Microsoft Windows. Licencje nie mogą mieć ograniczeń ilościowych dotyczących liczby obsługiwanych innych zasobów (np. drukarki, skanery, monitory itp). Ponadto musi posiadać co najmniej 1 licencje dostępową do konsoli zarządzającej.