***znak sprawy***: **BI.271.7.2020** Proszowice, 14.01.2021 r.

|  |  |  |
| --- | --- | --- |
| **ZMIANA SIWZ**  **w zakresie Załącznika A - OPZ**  **oraz terminu składania i otwarcia ofert** |  | **Gmina Proszowice**  **ul. 3 Maja 72**  **32-100 Proszowice** |

dotyczy: **postępowania prowadzonego w trybie przetargu nieograniczonego na** **dostawę i wdrożenie infrastruktury sprzętowo-programowej w ramach projektu pn.** **Cyfrowe Proszowice – nowoczesne zarządzanie w administracji realizowanego w ramach Regionalnego Programu Operacyjnego Województwa Małopolskiego na lata 2014-2020, II Osi Priorytetowej Cyfrowa Małopolska, Działanie 2.1 E-administracja i otwarte zasoby, Poddziałanie 2.1.1 Elektroniczna administracja**

**Na podstawie art. 38 ust. 4 ustawy** z dnia 29 stycznia 2004 r. – Prawo zamówień publicznych (Dz. U. z 2019 r. poz. 1843 z późn. zm.) **Zamawiający – Gmina Proszowice ul. 3 Maja 72, 32-100 Proszowice dokonuje zmiany SIWZ w zakresie:**

**ZAŁĄCZNIK A - SZCZEGÓŁOWY OPIS PRZEDMIOTU ZAMÓWIENIA**

**V. Opis przedmiotu zamówienia dla części nr 2.**

**pkt 16.** Oprogramowanie zarządzające oraz licencje dostępowe

**pkt. 17.** Oprogramowanie do monitorowania komputerów. Oprogramowanie dostarczone razem z serwerem musi zapewnić możliwość alarmowania, raportowania i monitorowania pracy komputera i użytkownika

**pkt. 18.** Oprogramowanie do szyfrowani poczty elektronicznej wraz z ochroną antiphishing o funkcjonalnościach

zostaje wykreślony i:

**Zastępuje się nowym pkt. 16, który otrzymuje brzmienie:**

16. Oprogramowanie zarządzająca oraz licencje dostępowe, Oprogramowanie do monitorowania komputerów. Oprogramowanie do szyfrowania.

1. Oprogramowanie dostarczone razem z serwerem musi zapewnić możliwość obsługi domeny, w tym funkcjonalności:
   1. zarządzania min. 100 użytkowników, grup oraz komputerów, urządzeń,
   2. zarządzania polisami GPO,
   3. obsługę profili użytkowników oraz profili mobilnych,
   4. obsługę min. 100 jednoczesnych podłączeń do serwera domeny,
   5. zarządzania użytkownikami, grupami, komputerami podpiętymi do kontrolera domenowego,
   6. możliwość tworzenia użytkowników i grup w kontrolerze domeny,
   7. nadawania haseł dla użytkowników w kontrolerze domeny,
   8. migracja użytkowników lokalnych do serwera domenowego działającego w systemie Windows
2. Architektura / budowa
   1. System musi umożliwić bezproblemową i stabilną obsługę co najmniej 2000 agentów jednocześnie.
   2. System musi posiadać następującą architekturę:
      1. Agent – komponent odpowiedzialny za zarządzanie komputerem, zbieranie danych oraz przesyłanie danych do serwera z wykorzystaniem bezpiecznego połączenia, pracujący w trybie usługi systemowej.
      2. Konsola administracyjna – przeznaczona do zarządzania całym systemem, w formie w pełni funkcjonalnej aplikacji internetowej (webowej). Pozwala na realizację pełnego zarządzania systemem oraz zasobami, wyposażona w mechanizmy do edycji/modyfikacji/usuwania i analizy danych, zawierająca mechanizmy raportowania (nie jest dopuszczalne stosowanie aplikacji webowej do przeglądania danych oraz innej aplikacji do wprowadzania/edycji danych).
      3. Serwer – oprogramowanie odpowiadające za utrzymywanie komunikacji i wymianę danych z agentami.
      4. Baza danych pracująca na silniku Microsoft SQL Server w wersjach wyspecyfikowanych poniżej.
      5. Wszystkie komponenty systemu muszą się aktualizować samodzielnie za pośrednictwem bezpiecznego połączenia z serwerami aktualizacji producenta systemu. Czas aktualizacji wszystkich komponentów systemu: serwer, konsola administracyjna, baza danych, agenci - nie może przekroczyć 24h od wydania przez producenta nowej wersji dowolnego komponentu. Agenci na komputerach muszą się zaktualizować samodzielnie w czasie nie dłuższym niż 1h od pobrania aktualizacji od producenta, przy czym aktualizacja agentów musi przebiegać w pełni automatycznie z wykorzystaniem funkcjonalności wbudowanej w system (bez użycia zewnętrznych narzędzi, np. MS Active Directory). W przypadku, gdy połączenie pomiędzy systemem a serwerem aktualizacji producenta nie jest dostępne musi być możliwość dokonania aktualizacji manualnie poprzez pobranie ze strony producenta paczki aktualizacyjnej w postaci jednego pliku z kompletną aktualizacją.
      6. System musi w sposób w pełni automatyczny z wykorzystaniem serwera aktualizacji producenta aktualizować wzorce aplikacji, pakietów, pomoc i inne wbudowane bazy wiedzy.
      7. Agent do działania nie może wymagać instalacji komponentów pomocniczych typu .NET Framework lub innych z wyłączeniem komponentów WMI.
      8. Agent musi być dostępny dla administratora z poziomu webowego interfejsu konsoli administracyjnej zawsze w najnowszej wersji wydanej przez producenta (bez konieczności pobierania go od producenta), w postaci pliku msi gotowego do zainstalowania (bez konieczności dodatkowego wykonywania zmian/ustalania parametrów) w pliku msi.
      9. System musi zezwalać na wygenerowanie instalatora agenta, który umożliwi użytkownikowi instalację usługi bez posiadania poświadczeń administrator.
      10. Agent musi być możliwy do zainstalowania za pośrednictwem MS Active Directory, za pomocą skryptów lub manualnie, poprzez uruchomienie na danej stacji roboczej.
      11. Agent musi pracować w trybie niewidocznym dla użytkownika (usługa systemowa).
      12. System powinien umożliwiać generowanie unikatowego identyfikatora agenta – wygenerowanego losowo i unikatowo (np. za pomocą mechanizmu typu GUID) lub w sposób powtarzalny dla danego komputera) na podstawie kombinacji parametrów wybranych przez użytkownika systemu spośród następujących: nazwy producenta BIOS, numeru seryjnego komputera, system UUID, nazwy komputera, dowolnego oraz losowego ciągu znaków.
      13. Agent musi mieć definiowalny priorytet pracy (ABOVE\_NORMAL, NORMAL, BELOW\_NORMAL, IDLE), przy czym w każdym momencie administrator może automatycznie z poziomu konsoli administracyjnej systemu wydać polecenie zmiany tej konfiguracji na dowolnej grupie komputerów.
      14. Agent musi wspierać do sześciu różnych adresów serwera rozumianych jako adresy w sieci lokalnej, rozległej (VPN) oraz za NATem i potrafić wykorzystać adres dostępny (na którym następuje połączenie z serwerem) w dowolnym momencie działania, bez konieczności restartu agenta.
      15. System musi umożliwiać komunikację pomiędzy agentami a serwerem w sieciach lokalnych, rozległych, także gdy komputery znajdują się za NATem.
      16. System musi mieć możliwość współpracy komponentów agent i serwer w taki sposób, aby serwer mógł współpracować ze wszystkimi poprzednimi wersjami agentów.
      17. System musi mieć wbudowane mechanizmy automatycznej konserwacji/utrzymania zgodnie ze zdefiniowanym harmonogramem realizujące co najmniej: usuwanie zbędnych danych z systemu (dane z monitoringu uruchamianych aplikacji, uruchamianych procesów, odwiedzonych stron www, wydrukowanych dokumentów, indeksowanie bazy danych, kopie bezpieczeństwa przyrostowe i nieprzyrostowe, zmniejszanie bazy danych. Harmonogram musi mieć możliwość ustalenia częstotliwości wykonywania zadania (godzina, dzień, tydzień, miesiąc), możliwość zmiany wartość parametrów wejściowych do wykonania danej konserwacji, a także zatrzymania/uruchomienia wybranych pozycji harmonogramu w dowolnym momencie. System musi prezentować historię przeprowadzonych konserwacji/utrzymania.
3. Wymagania systemowe:
   1. Konsola administracyjna musi działać w pełni responsywnie (niezależnie od wielkości i rozdzielczości ekranu urządzenia wyświetlającego) na dowolnej przeglądarce stron WWW zgodnej z HTML5 (np. Internet Explorer 11, Firefox, Chrome, Opera).
   2. Agent musi działać na systemach 32 i 64 bitowych: Windows Server2012/2012R2/2016/2019, Windows 7/8/8.1/10, MacOS 10.7/10.8, Linux dla wersji: Ubuntu v.11.04 lub wyższa, Debian v.6.0 lub wyższa, RedHat v.6.0 lub wyższa, CentOS v.6.0 lub wyższa, Fedora v.16 lub wyższa.
   3. Serwer musi działać na systemach 64 bitowych: Windows Server 2012/2012R2/2016/2019, Windows 7/8/8.1/10.
   4. Serwer www musi być oparty o platformę Microsoft 64 bit (Windows Server 2012/2012R2/2016/2019, Windows 10) oraz Java 8 (JRE lub JDK), Apache Tomcat 8+.
   5. Baza danych musi działać na silniku Microsoft SQL Server 2012/2014/2016/2017/2019 w wersji 64 bitowych zarówno komercyjnych jak i bezpłatnych (np. Microsoft SQL Server Express Edition).
   6. Jeśli architektura / wymagania systemu wymagają licencji typu CAL dla każdego komputera z zainstalowanym agentem należy dostarczyć wraz z systemem odpowiednią liczbę licencji CAL.
   7. System musi mieć możliwość pracy w środowisku wirtualnym Microsoft Hyper-V oraz VMWare.
4. Interfejsy
   1. System musi umożliwiać wielokrotny, zgodny z harmonogramem lub na życzenie, import użytkowników, komputerów, struktury organizacyjnej (całości bądź wybranego kontenera) z usługi MS Active Directory, przy czym import struktury organizacyjnej musi następować we wskazane miejsce struktury organizacyjnej zdefiniowanej w systemie.
   2. Import obiektów z MS Active Directory musi być odporny na zmianę nazw obiektów (nazwy użytkownika, struktury organizacyjnej itp.) – podczas import zmienione dane muszą zostać odpowiednio zaktualizowane wg klucza UUID.
   3. System musi umożliwiać wsparcie dla SSL i TLS podczas importu z Active Directory
   4. System musi umożliwiać import użytkowników z zewnętrznego pliku CSV.
   5. System musi posiadać wbudowany, w pełni definiowalny przez administratora interfejs do importu innych niż komputery urządzeń (np. pendrive, monitory, switche itp.) wraz z danymi o kosztach zakupu, nr dokumentu zakupowego, dostawcy, daty zakupu, gwarancji. Import musi umożliwiać pobieranie danych z dowolnego źródła danych o dowolnej strukturze danych z wykorzystaniem sterownika ODBC (np. z pliku tekstowego, pliku xls, bazy danych) w sposób jednorazowy lub zgodnie ze zdefiniowanym harmonogramem. Import aktualizuje te same dane wcześniej zaimportowane.
   6. System musi umożliwiać pobieranie danych z komputerów (wyników skanowania) metodą bezpośredniego połączenia, za pośrednictwem serwera pocztowego (MAIL), za pośrednictwem serwera HTTP/HTTPS.
5. Funkcjonalności systemu zarządzania infrastrukturą IT
   1. Funkcjonalność agenta
      1. System musi umożliwiać pełne zdalne zarządzanie agentami (w sposób masowy i jednostkowy) w zakresie: uruchamiania i wyłączania agenta, zmiany konfiguracji, uruchamiania skanowania, przekazania dowolnych zadań do wykonania (poleceń systemu operacyjnego), uruchamiania i wyłączania polityk w obszarze bezpieczeństwa (DLP).
      2. Agent musi mieć możliwość konfiguracji zakresu skanowania plików w oparciu o nazwę plików (z uwzględnieniem znaków wieloznacznych), lokalizację na konkretnym dysku, datę utworzenia pliku oraz wielkość
      3. Agent musi mieć możliwość wyświetlenia dowolnego komunikatu w postaci HTML wysłanego z poziomu konsoli administracyjnej a konsola musi udostępnić dane o dacie i godzinie wyświetlenia komunikatu oraz użytkowniku, który go wyświetlił.
      4. Agent musi mieć budowę modułową – uniemożliwienie pracy jednego z modułów (np. w wyniku niekompatybilnego systemu operacyjnego, pracy programów firm trzecich, awarii sprzętowej) nie może blokować pracy całego Agenta.
      5. Po wykryciu nieprawidłowości w pracy dowolnego z modułów Agent powinien podjąć samoczynną próbę jego naprawy i przywrócenia do działania.
   2. Funkcjonalność konsoli administracyjnej
      1. Konsola musi być w pełni polskojęzyczna.
      2. Interfejs konsoli musi być wyposażony w intuicyjne mechanizmy obsługi, musi zapewniać pełną obsługę funkcjonalną (dodawanie/modyfikacja/usuwanie).
      3. Konsola administracyjna musi być wyposażona w panel zawierający graficzne widgety prezentujące dane w postaci wykresu kołowego i słupkowego bądź w formie tabeli z danymi.
      4. Dane na widgetach muszą być aktualizowane automatycznie nie rzadziej niż 1 raz/ godzinę lub w każdym czasie na życzenia użytkownika.
      5. Widgety muszą być skojarzone dziedzinowo ze wszystkimi obszarami zarządzania infrastrukturą, a każdy obszar powinien być reprezentowany przez min. 5 widgetów (np. w obszarze zarządzania komputerami system powinien być wyposażony w widgety zawierające: ilość komputerów w ramach danego typu, ilość komputerów on/off-line, strukturę komputerów wg ilości pamięci RAM, ilość komputerów wg ilości wolnego miejsca na dysku, ilość komputerów wg dat ostatnich połączeń)
      6. Z każdego widgetu można uzyskać szczegółową informację analityczną (listę z danymi składającymi się na wybraną wartość na widgecie).
      7. System musi posiadać Security Dashboard prezentujący element pracy sieci, komputerów i użytkowników wpływające na bezpieczeństwo organizacji.
      8. Security Dashboard musi posiadać definiowalne przedziały czasu, struktury organizacji, typy wykresów oraz kolorystkę w dostępnych widżetach.
      9. Security Dashboard musi posiadać co najmniej 30 widżetów dostępnych dla użytkownika.
      10. System musi posiadać filtr roboczy, przeszukujący całą tabelę po zdefiniowanym słowie.
      11. System musi umożliwiać i zapamiętywać w profilu użytkownika indywidualną personalizację interfejsu konsoli administracyjnej (wybór wyświetlanych kolumn, ich kolejność, język, definiowanie filtrów, kolejność sortowania, wyświetlane widgety, ich konfigurację i kolejność).
      12. Dane prezentowane na wszystkich widokach/zakładkach w systemie muszą być dynamicznie filtrowane w oparciu o reguły utworzone przez dowolnego użytkownika systemu. Reguły muszą być zapamiętywane i dostępne w kolejnych sesjach oraz oparte co najmniej o: nazwę komputera, IP, rodzaj systemu operacyjnego, identyfikator agenta, strukturę organizacyjną, stan agenta (włączony/wyłączony), nazwę użytkownika zalogowanego, producenta sprzętu, dostawcę sprzętu, lokalizację komputera, dowolnie zdefiniowaną przez użytkownika wartość (np. kolor obudowy komputera). Użytkownik może wybrać za jednym razem więcej niż jedną regułę. Zmiana wybranej reguły powoduje aktualizację wyświetlonego widoku.
      13. System musi umożliwiać definiowanie poziomu uprawnień dla grupy oraz użytkownika (odczyt, dodawanie, usuwanie, modyfikowanie, wydruk) do wszystkich widoków danych oraz wybranych elementów struktury organizacyjnej, musi być wyposażony w opcję dziedziczenia uprawnień. Odebranie praw do widoku lub zakładki na widoku powoduje ukrycie opcji.
      14. Lista użytkowników / administratorów systemu musi być importowana i aktualizowana zgodnie z harmonogramem w oparciu o mechanizm RBAC (Role Base Access Control) z wybranego obiektu Active Directory. Użytkownik wyłączony/usunięty/zablokowany w Active Directory automatycznie traci prawa do korzystania z konsoli administracyjnej systemu.
      15. Konsola musi umożliwiać wykonywanie poszczególnych poleceń na wielu rekordach, w szczególności na wszystkich rekordach, również tych, które nie są widoczne w konsoli w ramach jednej strony (zaznacz wszystko).
      16. Konsola administracyjna musi zawierać szczegółowe informacje dotyczące pracy wszystkich komputerów: wersja agenta, stanu agenta (włączony/wyłączony), zalogowanego użytkownika, historii czasu włączenia i wyłączenia komputera.
      17. Konsola musi umożliwić bezpośrednie przejście do witryny internetowej producenta z poziomu repozytorium producentów (o ile taka jest dostępna, np. DELL).
      18. Konsola musi umożliwić bezpośrednie przejście do strony producenta zawierającej dodatkowe dane konfiguracyjne na temat konkretnego komputera w oparciu o Service Tag lub inny unikatowy identyfikator (np. Dell)
      19. Konsola musi zawierać w sobie pełną dokumentację systemu, dokumentacja musi być na bieżąco aktualizowana poprzez automatyczne mechanizmy aktualizacji z serwera aktualizacji producenta.
   3. Zarządzanie licencjami
      1. System musi umożliwiać zarządzanie licencjami w ramach dowolnego elementu struktury organizacyjnej (dla wybranej struktury organizacyjnej pokazuje liczbę instalacji i liczbę licencji w danym modelu licencjonowania wraz z listą komputerów).
      2. System musi dawać możliwość wykonywania (historia) wielu audytów legalności i zapamiętywać wyniki tych audytów w odniesieniu do systemów operacyjnych jak i aplikacji/pakietów, z uwzględnieniem segmentu struktury organizacyjnej.
      3. Zarządzanie oprogramowaniem musi następować z podziałem na aplikacje i pakiety oprogramowania.
      4. System musi pozwalać na zdefiniowanie dowolnej ilości tzw. „standardów oprogramowania”, które definiują 3 kategorie oprogramowania: „oprogramowanie standardowe” – pozycje z tej listy są wymagane do zainstalowania obowiązkowo na każdym komputerze, „oprogramowanie dodatkowe” - pozycje z tej listy mogą być zainstalowane (nie jest to wymagane) a instalacja odbywa się na wniosek samego użytkownika lub jego przełożonego, „oprogramowanie nieokreślone” – oprogramowanie nie należące do żadnej z dwóch powyżej zdefiniowanych kategorii a zidentyfikowane na komputerze.
      5. System umożliwia zdefiniowanie listy aplikacji zabronionych.
      6. System umożliwia utworzenie schematów (kolekcji) oprogramowania zabronionego i w momencie pojawienia się ich na komputerze przystępuje do automatycznego odinstalowania w trybie cichym (bez interfejsu).
      7. System zbiera szczegółowe informacje o systemie operacyjnym (wersja, edycja, service pack, poprawki, data instalacji).
      8. System umożliwia odczytywanie identyfikatorów i kluczy produktowych dla systemu operacyjnego oraz dowolnego oprogramowania, tam gdzie jest to tylko technicznie możliwe.
      9. System wspiera następujące typy licencji: Enterprise, Licensed concurrent, Licensed Name, Licensed per Processor, Licensed per Seat, Licensed per Server, OEM, OEM Downgrade, Open, Select, MOLP Open Value (Company wide), MOLP Open Value (non-Company wide), MOLP Open Value Subscription, CAL, SAAS, Trial, Shareware.
      10. System automatycznie klasyfikuje i rozlicza licencje OEM dla systemów operacyjnych oraz licencje typu freeware dla aplikacji.
      11. System musi pomijać w rozliczeniu licencje wygasłe (po terminie ważności) i informować administratora o wygasaniu licencji.
      12. System musi umożliwiać wyróżnianie licencji zabezpieczonych kluczami sprzętowymi.
      13. System automatycznie wskazuje liczbę posiadanych licencji oraz liczbę używanego oprogramowania (pokazuje braki oraz nadwyżki).
      14. System automatycznie uwzględnia i rozlicza licencje typu Upgrade i Downgrade wg zdefiniowanych przez użytkownika reguł.
      15. System prezentuje datę instalacji oprogramowania.
      16. System umożliwia ewidencję licencji (data zakupu, cena, dostawca, nr faktury, typ licencji, klucz produktowy, identyfikator produktowy, data wygaśnięcia, nr dokumentu OT, nr zapotrzebowania) poprzez rejestrację dokumentów źródłowych (faktur zakupu) z możliwością dołączenia dowolnych załączników z repozytorium.
      17. System umożliwia przypisanie licencji do użytkownika i/lub komputera oraz udostępnia informację o licencjach zarejestrowanych i jednocześnie wolnych (nieprzypisanych).
      18. System umożliwiać zbieranie informacji na temat uruchamianych aplikacji na inwentaryzowanych komputerach (m.in. czas uruchomienia, nazwa zalogowanego użytkownika, nazwa aplikacji). System musi posiadać mechanizm zabezpieczający przed powstaniem niekompletnych lub niewłaściwych zapisów w wyniku braku zasilania lub innych awarii inwentaryzowanego systemu/sprzętu).
      19. System musi udostępniać informację o uruchamianych aplikacjach w okresie 3/6/12 miesięcy oraz udostępniać datę ostatniego uruchomienia.
      20. System musi automatycznie wyliczać przybliżone oszczędności z zakupionych a nie zainstalowanych aplikacji, przybliżone oszczędności z zainstalowanych a niewykorzystanych licencji oraz przybliżone nakłady konieczne na uzyskanie pełnej legalności.
      21. System musi umożliwiać podgląd historii zmian aplikacji i pakietów na komputerach.
      22. System musi umożliwiać zdalne odinstalowanie oprogramowania na jednym bądź wybranych komputerach.
      23. System musi udostępniać informacje o stopniu wykorzystania aplikacji / pakietów dla modeli licencjonowania oprogramowania typu CAL w podziale na analizę godzinową/dzienną/miesięczną w zadanym okresie czasu. W/w informacja winna być przedstawiona również w postaci graficznej.
      24. System musi udostępniać informacje o stopniu wykorzystania oprogramowania typu web dla modeli licencjonowania oprogramowania typu CAL w podziale na analizę godzinową/dzienną/miesięczną w zadanym okresie czasu. W/w informacja winna być przedstawiona również w postaci graficznej.
   4. Wzorce aplikacji i pakietów
      1. System ma posiadać wbudowaną bazę wzorców dostawcy oprogramowania posiadającą co najmniej 3,8 tys. wzorców aplikacji, 1,5 tys. producentów, 21 tys. plików, 1,5 tys. wbudowanych treści umów licencyjnych różnych producentów oprogramowania.
      2. System musi udostępniać informacje dotyczące plików, na podstawie których zidentyfikowana została dana aplikacja.
      3. System musi prezentować informacje o ilości i dacie publikacji posiadanej bazy wzorców oprogramowania.
      4. System musi posiadać możliwość definiowania własnych wzorców aplikacji i pakietów (składających się z aplikacji) w oparciu o definiowalne reguły rozpoznawania.
      5. Własne wzorce aplikacji i pakietów muszą mieć pierwszeństwo w procesie rozpoznawania aplikacji i pakietów.
      6. System musi mieć możliwość zamawiania bezpośrednio z poziomu konsoli administracyjnej u producenta systemu wzorców oprogramowania z możliwością wskazania dla jakiego komputera / komputerów wzorce mają być utworzone. Zamówione i utworzone przez Producenta wzorce muszą automatycznie (bez ingerencji administratora systemu) zostać zaimportowane do systemu.
      7. System musi rozpoznawać wersję i edycję zainstalowanych pakietów Microsoft Office (tam gdzie jest to technicznie możliwe (np. Microsoft Office 2007 Professional, Microsoft Office 2007 Standard, Microsoft Office 2003 Standard itd.).
   5. Inwentaryzacja sprzętu komputerowego
      1. System musi umożliwiać: automatyczną inwentaryzację komputerów znajdujących się w sieci lokalnej oraz komputerów znajdujących się poza siecią lokalną (za NATem).
      2. System musi zbierać szczegółowe informacje o sprzęcie (producent, model, data produkcji, numer seryjny) w oparciu o klasy WMI (Windows Management Instrumentation). Szczegółowość odczytywania danych musi być parametryzowana za pomocą definiowanego zapytania w standardzie WMI Query Language.
      3. System ma umożliwiać skanowanie kości pamięci RAM (z podaniem jednoznacznej specyfikacji kości, typu, numeru seryjnego oraz informacji o taktowaniu).
      4. System ma odczytywać informacje o zainstalowanych kościach pamięci: producent, numer seryjny (Serial Number), numer części (Part Number), rozmiar, częstotliwość, taktowania.
      5. System musi mieć możliwość odczytywania danych z dowolnego miejsca rejestru systemowego. Musi istnieć możliwość łączenia (konkatenacji) kilku pozycji z różnych miejsc rejestru oraz możliwość automatycznego, rekurencyjnego wyszukiwania wartości podanego klucza począwszy od wskazanego miejsca w hierarchii kluczy rejestru.
      6. System ma umożliwiać automatyczne skanowanie monitorów podłączonych do komputera (ze wskazaniem producenta, modelu, numeru seryjnego, przekątnej ekranu).
      7. System ma umożliwiać skanowanie dysków twardych (z podaniem typu interfejsu, numeru seryjnego oraz informacji SMART).
      8. System musi umożliwić budowanie powiadomień administracyjnych w oparciu o dowolne atrybuty tabeli SMART dysku.
      9. System musi umożliwiać skanowanie uprawnień użytkowników oraz grup użytkowników wraz z informacją o uprawnieniach, czy konto jest włączone, zablokowane, czy wymagana jest zmiana hasła, czy hasło wygasa, czy hasło jest wymagane).
      10. System prowadzi szczegółową ewidencję zmian konfiguracji sprzętu.
      11. System udostępnia informacje o występowaniu plików na komputerach (nazwa, rozmiar, rodzaj, wielkość, lokalizacja, w przypadku plików wykonywalnych: wersja, producent).
      12. System musi umożliwiać dokonanie klasyfikacji pliku wg dowolnie zdefiniowanych kategorii (np. audio, wideo, graficzne, erotyczne/pornograficzne, archiwa, wykonywalne.
      13. System pozwala na zdalne trwałe (bez możliwości odzyskania) usunięcie dowolnego pliku/plików na dowolnie zdefiniowanej grupie komputerów.
      14. System udostępnia informacje o zmianach w systemie plików (dodano plik, usunięto plik)
      15. System umożliwia dodawanie notatek do każdej pozycji sprzętu.
      16. System musi umożliwiać ewidencję zdarzeń serwisowych dowolnego typu (np. naprawy sprzętu, wymiany części).
      17. System musi pozwalać na dołączanie do urządzeń dokumentów z repozytorium.
      18. System umożliwia samodzielną definicję, ewidencję oraz wydruk wszelkiego typu protokołów (przyjęcie, przekazanie do użytkowania, likwidacja).
   6. Inwentaryzacja urządzeń podłączanych do komputera
      1. System automatycznie identyfikuje i klasyfikuje urządzenia podłączane do komputera (pendrive, kamera, aparat, monitor zewnętrzny, pamięć masowa, telefon, urządzenie multimedialne itp.
      2. System pozwala na automatycznie lub ręczne przypisanie podłączonego urządzenia do komputera oraz użytkownika.
      3. System ewidencjonuje historię podłączanych urządzeń zewnętrznych w zakresie: komputer, data, godzina, kto podłączył, czy urządzenia było podłączane na innym komputerze, czy urządzenie było podłączane przez innego użytkownika).
   7. Identyfikacja środowisk wirtualizacji
      1. System musi być wyposażony w skaner środowisk wirtualizacji Hyper-V oraz VMware.
      2. Skaner środowisk wirtualizacji musi być w pełni programowalny, musi obsługiwać wiele środowisk wirtualizacji oraz dowolną ilość atrybutów logowania (login, hasło).
      3. Skaner środowisk wirtualizacji musi być wyposażony w programowalny harmonogram skanowania.
   8. Inwentaryzacja urządzeń innych niż komputery
      1. System musi umożliwiać inwentaryzację manualną (ewidencję) sprzętu innego niż komputery: np. drukarki, switche, routery, monitory, pamięci masowe itp.
      2. System musi być wyposażony we wbudowany, konfigurowalny w zakresie IP oraz portów, pracujący zgodnie z harmonogramem skaner SNMP. Skaner musi wykryć typ urządzenia na danym IP/porcie i zwracać podstawowe informacje o tym urządzeniu (nazwa, producent, opis).
      3. Skaner SNMP musi kojarzyć (łączyć) zinwentaryzowane urządzenia (np. komputery, drukarki) z danymi uzyskanymi w procesie skanowania IP/port.
      4. System musi zbierać dane o jakości połączenia: czas odpowiedzi serwisów (usług) podawany w milisekundach: średni czas odpowiedzi, minimalny czas odpowiedzi, maksymalny czas odpowiedzi, ilość dostarczonych informacji – pakietów dostarczonych, straconych oraz procent strat.
      5. System musi być wyposażony we wbudowany, konfigurowalny skaner sieci, pozwalający na monitorowanie aktywnych usług oraz zweryfikowanie czy znalezione skanerem komputery posiadają agenta, a w przypadku, gdy takiego agenta nie posiadają powinien umożliwić zdalną instalację agenta.
      6. System musi posiadać możliwość niezwłocznej i automatycznej identyfikacji podłączonych urządzeń.
      7. Baza wzorców systemu musi zawierać min. 120 monitorowanych portów i usług.
      8. System musi posiadać możliwość generowania map sieci bazujących na danych zebranych ze skanowania sieci.
      9. System musi umożliwiać generowanie map według dowolnych filtrów użytkownika.
      10. System musi obsługiwać komunikaty syslog.
      11. System musi posiadać możliwość monitorowania serwerów WWW i adresów URL.
      12. System umożliwia wprowadzanie dowolnych notatek oraz zdarzeń serwisowych.
      13. System musi monitorować zmiany ewidencyjne i ruchy sprzętu.
      14. System musi umożliwiać przypisanie urządzenia do użytkownika, ewidencję napraw, gwarancji.
      15. System musi mieć możliwość przypominania o upływającym terminie gwarancji.
      16. System musi pozwalać na dołączanie do urządzeń dokumentów z repozytorium wewnętrznego systemu.
      17. System udostępnia informację o wartości wprowadzonego sprzętu.
      18. System musi umożliwiać samodzielną definicję, ewidencję oraz wydruk wszelkiego typu protokołów oraz zapewniać automatyczną numerację tych dokumentów zapewniającą unikatowość.
      19. System musi pozwalać na kopiowanie (duplikację) dowolnego urządzenia dowolną ilość razy.
      20. System musi pozwalać na ewidencję umów utrzymaniowych (SLA) w odniesieniu do zaewidencjonowanych licencji oraz urządzeń w zakresie co najmniej: nazwa, okres, data dokumentu, numer dokumentu, dostawca, osoba kontaktowa, wartość, opis, warunki oraz umożliwiać dołączenie dowolnej ilości załączników z repozytorium i powiązanie umowy utrzymaniowej z dowolną ilością zasobów (urządzenia, licencje).
   9. Ochrona danych (DLP)
      1. System automatycznie tworzy bazę danych podpinanych do komputerów urządzeń USB.
      2. System automatycznie klasyfikuje podłączane urządzenia (pamięć masowa, pendrive, aparat fotograficzny, urządzenie multimedialne itp.)
      3. System umożliwia uzyskanie informacji kto, kiedy i na jakim komputerze posługiwał się urządzeniem zewnętrznym, pozwalając na jego jednoznaczne zidentyfikowanie.
      4. System umożliwia utworzenie listy urządzeń USB dozwolonych do stosowania - tzw. białej listy urządzeń USB.
      5. System ma możliwość zidentyfikowania urządzenia USB i wprowadzenia go do systemu za pośrednictwem konsoli administracyjnej oraz wbudowanego do konsoli oprogramowania/skryptu, pozwalając na zidentyfikowanie jednocześnie wielu urządzeń USB (multiplekser USB).
      6. System musi umożliwiać zdefiniowanie reguł stanowiących podstawę użytkowania urządzeń USB (dozwolone/niedozwolone) na inwentaryzowanych komputerach wg kryteriów: użytkownik, dzień tygodnia, okres (data od, godzina od, data do, godzina do), urządzenie USB, komputer, data obowiązywania reguły.
   10. Zdalna administracja komputerami
       1. System ma automatyczne wykonywać dowolne polecenia na dowolnych komputerach: wykonywanie poleceń powłoki, uruchamianie aplikacji, instalacja/deinstalacja oprogramowania, zmiany w rejestrach systemowych (dodawanie, usuwanie, modyfikowanie), usuwanie oraz kopiowanie plików i folderów, dostarczanie wyników zwróconych przez wykonane zadanie do bazy danych i prezentowanie ich w konsoli zarządzającej, możliwość wykonywania zadań z uprawnieniami dowolnego użytkownika.
       2. System musi posiadać wbudowany skaner wyposażony w harmonogram skanowania umożliwiający wykrywanie (rozpoznawanie) komputerów z technologią Intel VPro/AMT wraz z identyfikacją IP technologii Vpro, portu VPro oraz wersji Vpro.
       3. System musi umożliwiać zarządzanie komputerami z technologią Intel vPro, w tym: Serial Over LAN, zdalne włączanie, wyłączanie komputera, zdalna konfiguracja BIOS, uruchomienie zdalnie komputera przy użyciu obrazu ISO lub IMG znajdującego się w dowolnej lokalizacji.
       4. System ma umożliwiać połączenie się z wybranym komputerem w trybie graficznym (od VPro v.6).
       5. System musi umożliwiać za pomocą technologii Ultra VNC: przejęcie ekranu, klawiatury i myszki użytkownika, blokadę klawiatury i myszki, zdalne uruchamianie aplikacji, zarządzanie usługami i restart komputera, zdalną instalacja oprogramowania, poprawek i aktualizacji (service pack, patch).
       6. System umożliwia zdalne podłączenie do wielu komputerów jednocześnie i podgląd oraz operowanie na pulpitach tych komputerów w technologii Ultra VNC.
       7. System musi umożliwiać uruchomienie do 6 sesji Ultra VNC na jednym ekranie.
       8. System musi umożliwiać za pomocą technologii WebRTC: przejęcie ekranu, przejęcie ekranu po zgodzie użytkownika, zarządzanie aplikacjami i usługami, uśpienie, restart wyłączenie komputera, skróty klawiszowe (Ctrl+Alt+Del, Alt+F4, Alt-Tab, Ctrl+W, Shift+Win+M, Win, Win+Down, Win+Up, Win+Left, Win+Right, Win+L, Win+M, Win+R), schowek.
       9. System musi umożliwiać przy wykorzystaniu technologii WebRTC obsługę konsoli Windows (Wiersz poleceń/CMD) oraz operacje na plikach (kopiowanie, usuwanie, tworzenie nowych folderów, zmianę nazwy, wycinanie) w czasie rzeczywistym bez potrzeby zdalnego połączenia do komputera, a wszystkie operacje są logowane i dostępne w systemie.
       10. System umożliwia zdalne połączenie do wielu komputerów jednocześnie i podgląd oraz operowanie na pulpitach tych komputerów w technologii WebRTC
       11. System musi umożliwiać uruchomienie do 6 sesji WebRTC na jednym ekranie.
       12. Funkcjonalności technologii WebRTC muszą działać w sieci lokalnej oraz poza NATem.
       13. System musi posiadać predefiniowane zadania (polecenia) możliwe do wykonania zdalnie – niezwłocznie lub zgodnie z harmonogramem o funkcjonalnościach typowego harmonogramu windows; zadania powinny być podzielone na typy: administracyjne, bezpieczeństwo, konserwacyjne a użytkownik może utworzyć dowolny nowy typ zadania.
       14. Minimalne zadania predefiniowane: wyświetlanie aktywnych połączeń sieciowych, czyszczenie buforu DNS, pobranie listy zalogowanych użytkowników, ping, tracert, pobranie listy procesów, wyłączenie/włączenie komputera, wyłączenie/włączenie usługi, wyłączenie/włączenie/restart zapory windows, włączenie usługi Windows Update, pobranie zmiennych środowiskowych, opróżnienie kosza, usunięcie plików tymczasowych, wymuszenie sprawdzenia dostępności aktualizacji Windows Update, wymuszenie aktualizacji zasad grup (AD), konserwację dysku twardego.
       15. Każde wykonanie zadania musi mieć odzwierciedlenie w statusie wykonania zadania (poprawne, z błędem) oraz udostępniać informację zwrotną o przebiegu wykonania (godzina, data, status).
       16. System musi umożliwiać zdefiniowanie dowolnego własnego zadania z poziomu konsoli administracyjnej z wykorzystaniem poleceń cmd, windows powershell. System musi posiadać co najmniej 70 predefiniowanych udokumentowanych poleceń administracyjnych.
   11. Automatyzacja
       1. System ma mieć możliwość ustalania harmonogramu, zgodnie z którym uruchamiane są czynności konserwacyjne, naprawcze, porządkujące.
       2. Harmonogram musi mieć możliwość ustalenia częstotliwości wykonywania danej czynności (godzina, dzień, tydzień, miesiąc), możliwość zmiany wartość parametrów wejściowych, a także zatrzymania/uruchomienia harmonogramu uruchomienia dla każdej z czynności.
       3. System musi mieć możliwość definiowania czynności wykonywanych automatycznie.
       4. System musi być wyposażony w następujące mechanizmy automatyzacji: wykonywanie kopii bezpieczeństwa bazy danych, identyfikacja aplikacji i pakietów, porządkowanie bazy danych / odbudowa indeksów, usuwanie nadmiarowych danych w bazie danych, usuwanie zewnętrznych plików (logów).
       5. System musi być wyposażony w mechanizmy informowania - wysyłania komunikatów (alerty) o: zasobach zakazanych (pliki erotyczne i pornograficzne), zasobach multimedialnych (pliki multimedialne), nowych komputerach w bazie danych, braku skanowania komputerów, brakach w licencjach, niewłaściwych datach systemowych komputerów, urządzeniach bez użytkowników, zdublowanych systemach operacyjnych, zakazanych procesach/stronach www /aplikacjach, wygasaniu serwisu lub licencji, przekroczeniu wielkości bazy danych, nadmiernym obciążeniu dysków twardych, nadmiernym obciążeniu sieci, nadmiernym obciążeniu sieci na komputerze, nadmiernym obciążeniu procesora, nadmiernym obciążeniu pamięci RAM, małej ilości wolnego miejsca na dysku, upływającej gwarancji,
       6. System musi wspierać obsługę dowolnych poleceń powłoki na stacjach roboczych (kopiowanie plików, usuwanie plików, przenoszenie plików, zmiana ustawień systemu, wykonywanie programów, instalacja oprogramowania, instalacja poprawek itp.).
       7. System musi umożliwić wykonanie poleceń z uprawnieniami dowolnego użytkownika (Uruchom jako)
       8. System musi umożliwiać tworzenie zadań cyklicznych dla komputerów.
       9. Obsługa zadań cyklicznych musi następować w cyklu dziennym: co n dni, w każdy dzień powszedni, nowe zadanie n dni od wykonania, tygodniowym: w wybrane dni co n tygodni, nowe zadanie n tygodni od wykonania, miesięcznym: co x miesięcy n-tego dnia, pierwszy/drugi/trzeci/czwarty/ostatni poniedziałek/wtorek/środa/czwartek/piątek/sobota/niedziela/dzień wolny/dzień powszedni co n miesięcy, nowe zadanie n miesięcy od wykonania, rocznym: n dzień w wybranym miesiącu, w pierwszy/drugi/trzeci/czwarty/ostatni, w dowolny dzień tygodnia, dzień wolny/dzień powszedni wybranego miesiąca, nowe zadanie n lat od wykonania.
       10. System musi obsługiwać zadania cykliczne: bez daty końcowej, z końcem cyklu po n wystąpieniach, z końcem cyklu w określonej dacie.
   12. Zarządzanie magazynem IT
       1. System musi umożliwiać obsługę magazynu IT.
       2. System musi umożliwiać obsługę dowolnej ilości magazynów w różnych lokalizacjach.
       3. System musi umożliwiać obsługę dokumentów PZ, WZ, MM+, MM-, LI.
       4. System musi prowadzić ewidencję materiałów w magazynach w oparciu o metodę FIFO (pierwsze przyszło pierwsze wyszło).
       5. System musi umożliwiać obsługę kodów kreskowych dla materiałów w magazynach.
       6. System musi udostępniać informację o wartościach materiałów w poszczególnych magazynach, stanach materiałów w magazynach, dokumentach dotyczących danego materiału w dowolnym magazynie.
   13. Repozytorium
       1. Konsola administracyjna musi być wyposażona w repozytorium dokumentów dowolnego typu.
       2. Repozytorium musi umożliwiać: dodawanie nowych dokumentów dowolnego typu, przeszukiwanie, oznaczanie dokumentów (znaczniki TAG) więcej niż jednym znacznikiem, podgląd dokumentów, dołączanie dokumentów z repozytorium w dowolnym miejscu systemu, uzyskanie informacji w jakich miejscach systemu dany dokument repozytorium występuje.
   14. Kody kreskowe
       1. System wspiera obsługę kodów kreskowych jedno i dwuwymiarowych.
       2. System wspiera parametryzację kodu w zakresie wielkości graficznej kodu.
       3. System pozwala w każdym momencie na zmianę typu i atrybutów kodu.
       4. System informuje o błędzie generacji kodu, np. na skutek niewłaściwej długości wprowadzonego ciągu znaków w stosunku do danego standardu kodu.
       5. Istnieje możliwość podglądu kodu oraz jednostkowego i masowego wydruku kodu / kodów.
       6. System musi generować kody kreskowe (jedno i dwuwymiarowe) dla każdego zaewidencjonowanego urządzenia w standardzie wybranym przez użytkownika: aztec, codabar, code128, code39, dataMatrix, EAN128, EAN13, EAN8, interleaved2of5, ITF14, PDF417, POSTNET, qrcode, royalMailCBC, UPCA, UPCE, USPSIntelligentMail.
       7. Obsługa kodów kreskowych nie może wymagać instalacji czcionek.
       8. Parametry kodu kreskowego (wymiary, wielkość i typ czcionki) muszą być definiowalne.
       9. System musi umożliwiać współpracę z zewnętrznymi czytnikami kodów.
   15. Edukacja pracowników
       1. System musi mieć możliwość zdefiniowania pakietów tekstowych (kontent) celem automatycznego wysyłania do urządzeń i użytkowników komputerów.
       2. System musi posiadać predefiniowane szkolenia: „Klasyfikowanie informacji stanowiących tajemnicę przedsiębiorstwa”, „Kontrola zabezpieczeń i obiegu informacji stanowiących tajemnicę przedsiębiorstwa”, „Postępowanie w przypadku naruszenia tajemnicy”, „Udostępnienie informacji stanowiących tajemnicę”.
       3. Formatowanie treści musi być zgodne z HTML.
       4. System musi mieć możliwość edycji treści (zmiana kolejności, usuwanie, dodawanie nowych).
       5. System musi mieć programowalny harmonogram wysyłania treści do dowolnej grupy odbiorców.
       6. Użytkownik otrzymujący wiadomość musi być powiadamiany wizualne i dźwiękowo o otrzymaniu nowej wiadomości.
       7. Użytkownik musi mieć możliwość natychmiastowego odczytania wiadomości lub jej odłożenia (na 10 minut, 1, 2 lub 4 godziny) celem późniejszego odczytania.
       8. System musi posiadać zabezpieczenie (np. synchronizowany z serwerem znacznik czasowy) odporne na zmiany czasu na lokalnym komputerze (użytkownika) a pozwalające na jednoznaczne ustalenie daty i godziny dostarczenia i odczytania wiadomości.
       9. System musi udostępnia historię przesyłania wiadomości i odczytywania wiadomości przez użytkowników.
       10. System musi generować elektroniczną listę uczestników przeszkolonych (z odczytanym całym szkoleniem).
       11. System musi posiadać możliwość eksportu / importu treści.
   16. Monitorowanie wydruków
       1. System musi posiadać możliwość ewidencji wszystkich generowanych wydruków niezależnie od miejsca ich generowania oraz typu drukarki (lokalna, sieciowa).
       2. Ewidencja wydruków musi obejmować: nazwę i wielkość dokumentu, datę i godzinę wydruku, nazwę użytkownika drukującego, IP i nazwę komputera z którego dokonano wydruku, format dokumentu, informację i jedno bądź dwustronnym wydruku, informację o wydruku mono/kolor.
       3. System dla każdego wydruku, dla każdej drukarki musi obliczać rzeczywisty koszt wydruku w oparciu o wbudowany cennik wydruków obejmujący cenę papieru (w zależności od formatu) oraz cenę materiałów eksploatacyjnych (toner, tusz) dla danej drukarki, typu wydruku, rozmiaru papieru.
       4. System musi generować zestawienia pozwalające ustalić miejsca powstawania kosztów wydruków (komórki organizacyjne, użytkownicy) oraz stopień obciążenia poszczególnych urządzeń drukujących.
       5. System musi prognozować ilość i koszt wydruków na wszystkich drukarkach w okresie kolejnych 3,6,12 miesięcy.
       6. System musi pozwalać na grupowanie (kojarzenie) drukarek wg sterowników.
   17. Monitorowanie stron www
       1. System musi posiadać możliwość monitorowania odwiedzanych stron www niezależnie od typu używanej przeglądarki internetowej.
       2. Ewidencja otwieranych stron musi dotyczyć wielu jednocześnie otwartych zakładek.
       3. Ewidencja otwieranych stron musi działać również, gdy otwierana jest strona z połączeniem szyfrowanym (https).
       4. Ewidencja musi obejmować co najmniej: nazwę i adres IP komputera, nazwę użytkownika, datę i godzinę, adres strony.
   18. Klasyfikator stron internetowych
       1. System musi posiadać automatyczny mechanizm klasyfikacji stron internetowych w oparciu o zawartość treści strony.
       2. System musi posiadać następujące możliwości klasyfikacji stron: wyłudzająca dane, zablokowana przez rząd, wyłudzająca dane, niebezpieczna struktura strony, strona wczytująca zasoby z zewnętrznych serwerów, produktywna/nieproduktywna, bez certyfikatu SSL.
       3. Baza danych klasyfikatora musi być na bieżąco (min. 1 /godz.) synchronizowana z rządową bazą danych stron zakazanych (Rejestr Domen Służących do Oferowania Gier Hazardowych) oraz z bazą danych CERT (lista ostrzeżeń zawierająca wykaz witryn stanowiących zagrożenie).
       4. Każda uruchamiana strona www musi zostać przypisana do jednej kategorii, przy czym kategoria ustawiona przez klasyfikator może być dowolnie zmodyfikowana przez administratora.
       5. Liczba predefiniowanych kategorii stron klasyfikatora musi wynosić min. 20 a liczba obsługiwanych języków min. 40, w tym język polski.
       6. System klasyfikacji musi poprawnie i automatycznie identyfikować język strony a proces klasyfikacji strony musi uwzględniać specyfikę językową strony.
       7. Baza wstępnie sklasyfikowanych stron w momencie instalacji systemu musi wynosić min. 4 mln stron i musi być na bieżąco w pełni automatycznie aktualizowana (min. raz/ dobę), przy czym strony te muszą pochodzić z podmiotów mających siedzibę na terenie Polski.
   19. Monitorowanie dziennika zdarzeń
       1. System musi posiadać możliwość monitorowania dziennika zdarzeń wszystkich komputerów.
       2. Ewidencja zdarzeń musi następować w oparciu o definiowalną kategorię zdarzenia: critical, error, warning, info, audit failure, audit success, debug oraz typ dziennika: aplikacja, bezpieczeństwo, system.
       3. System musi pozwalać na zdefiniowanie ewidencji zdarzeń z komputerów na podstawie kategorii zdarzenia.
       4. Ewidencja musi zawierać: datę i godzinę zdarzenia, nazwę i adres IP komputera, typ zdarzenia, opis zdarzenia.
   20. Monitorowanie pracy komputerów
       1. System musi posiadać możliwość monitorowania daty włączenia i wyłączenia komputera niezależnie czy znajduje się w sieci lokalnej czy też poza nią i prezentować czas pracy komputera w układzie graficznym.
       2. System musi posiadać ewidencję daty i godziny przyłączenia i odłączenia komputera od systemu monitorującego.
       3. System musi ewidencjonować zdarzenia związane z logowaniem się użytkowników do danego komputera, również w przypadku podłączania się wielu użytkowników jednocześnie
   21. Monitorowanie sesji zdalnych połączeń
       1. System musi prowadzić ewidencję sesji zdalnych połączeń na każdym komputerze.
       2. Informacja o nawiązanej sesji musi zawierać co najmniej: nazwę i adres IP komputera z którego nastąpiło połączenia, nazwę użytkownika nawiązującego połączenie, nazwę i adres IP komputera docelowego, adres portu połączenia.
   22. Raportowanie i eksport danych
       1. Systemu musi umożliwiać wyeksportowania wybranych lub wszystkich danych do formatu xls, csv, OpenOffice calc, html, mht, xml, jpeg, png, gif, bmp.
       2. System musi mieć możliwość kategoryzowania raportów (spośród wszystkich raportów) oraz dodawania raportów użytkownika (zaprojektowanych przez użytkownika).
       3. System musi umożliwiać generowanie raportów bezpośrednio z każdego widoku w aplikacji z zastosowaniem bieżących filtrów.
       4. Generowanie raportu musi odbywać się po stronie serwera a nie klienta.
       5. System musi umożliwiać wieloinstancyjność raportowania (wiele otwartych raportów jednocześnie z wielu widoków).
       6. System musi mieć możliwość generowania i wyświetlania dowolnych wieloparametrycznych raportów w standardzie SAP Crystal Reports (rpt).
       7. System musi umożliwiać eksport danych z raportu do formatów: RPT, PDF, XLS, DOC, RTF.
       8. System musi obsługiwać raporty parametryczne z parametrami statycznymi (wprowadzanymi w momencie generowania raportów) oraz dynamicznymi (pobieranymi z bazy danych w momencie generowania raportu).
       9. System musi posiadać co najmniej 150 zdefiniowanych raportów dotyczących wszystkich obszarów funkcjonalnych.
       10. System musi posiadać możliwość ustalenia harmonogramu umożliwiającego cykliczne wysyłanie raportów w formacie co najmniej PDF oraz zapisywanie ich w dowolnym miejscu.
6. Bezpieczeństwo
   1. System musi być wyposażony w mechanizmy definicji praw dostępu do poszczególnych widoków danych i opcji w konsoli administracyjnej.
   2. Uwierzytelnianie do systemu musi być realizowane:
      1. Z wykorzystaniem imiennego konta użytkownika i hasła;
      2. Z wykorzystaniem imiennego konta administratorów aplikacji i hasła;
      3. Hasła w systemie i bazach danych nie mogą w żadnym z przypadków występować w formie jawnej;
      4. Za pośrednictwem jednokrotnego uwierzytelniania poprzez Active Directory;
      5. Za pośrednictwem jednokrotnego uwierzytelniania poprzez CAS.
   3. Siła hasła użytkownika musi być definiowalna w systemie w zakresie atrybutów: ilość znaków, ilość liter, ilość znaków specjalnych, ilość małych znaków, ilość wielkich znaków, ilość cyfr, ilość znaków specjalnych, ilość znaków alfanumerycznych, lista dopuszczalnych znaków specjalnych, lista wyłączonych znaków).
   4. Przechowywanie haseł administratorów w bazie danych musi być poddane odpowiednio wysokiemu zabezpieczeniu. Hasła muszą być zapisywane jako base64 z (sól + SHA512 z login + hasło).
   5. Prawa dostępu muszą opierać się na grupach i użytkownikach w zakresie: przeglądanie / edycja / usuwanie/ eksport.
   6. System musi udostępniać historię korzystania z poszczególnych opcji przez wybranych użytkowników/administratorów.
   7. System musi posiadać wbudowany mechanizm automatycznej synchronizacji czasu pomiędzy agentami oraz serwerem, gdzie wzorcowy czas jest po stronie serwera.
   8. System musi posiadać mechanizmy automatycznego wykonywania kopii bezpieczeństwa w zadanych interwałach czasowych w formie kopii przyrostowej i nieprzyrostowej oraz udostępniać informacje o rezultacie wykonania kopii.
   9. System musi pobierać dane z widoków (view) zdefiniowanych w bazie danych a nie bezpośrednio z tabel bazy danych.
   10. W przypadku wystąpienia awarii systemu i konieczności instalacji systemu na nowo system musi automatycznie z serwera aktualizacji producenta w ciągu 24 godzin dokonać aktualizacji wszystkich komponentów (konsola administracyjna, agenci, serwer, baza danych, bazy wiedzy).
   11. System musi być wyposażony w mechanizmy powtórnego załadowania danych historycznych pochodzących od agentów.
   12. System musi umożliwiać podłączenie i pracę certyfikatu SSL do konsoli webowej.
   13. System musi zapewniać:
       1. Pełne logowanie błędów w celu weryfikowania nieprawidłowości.
       2. Przechowywanie logów systemowych.
       3. Przechowywanie logów bezpieczeństwa.
       4. Przechowywanie logów aktywności użytkowników i administratorów.
       5. Pobieranie logów z agentów z poziomu konsoli administracyjnej.
       6. Możliwość eksportu logów.
       7. Definiowanie maksymalnego czasu przechowywania plików log.
   14. System musi zapewniać mechanizmy zapewniające integralność, poufność i dostępność przechowywanych informacji.
   15. System musi prezentować główne parametry infrastruktury IT związane z bezpieczeństwem, m.in.: podgląd bieżących alertów systemowych, aktualną ilość komputerów online / offline, monitorowanie niedozwolonych działań np. podłączenie nieautoryzowanych urządzeń oraz instalowanie niedozwolonego oprogramowania.
   16. Dane muszą być prezentowane w postaci graficznych widżetów, konfigurowanych przez użytkownika (format i kolor wykresu) w kategoriach: system operacyjne, komputery (jednostki), oprogramowanie, użytkownicy, sieć, sprzęt.
7. Wsparcie i pomoc
   1. System musi posiadać wbudowaną dokumentację w postaci min. 20 filmów instruktażowych w języku polskim.
   2. System musi posiadać wbudowaną dokumentację pomocy użytkownika w języku polskim.
   3. System musi posiadać podpowiedzi dziedzinowe (porady) w obszarze licencjonowania.
   4. Pomoc techniczna musi być świadczona co najmniej w dni robocze w godzinach od 8.00-16.00.
8. Szyfrowanie komputerów
   1. System musi identyfikować partycje dysków twardych zaszyfrowane BitLockerem.
   2. Szyfrowanie musi posiadać wbudowane mechanizmy do masowego zdalnego szyfrowania BitLockerem i wspierać metody XTS\_AES\_256, XTS\_AES\_128, AES\_256, AES\_128 oraz typy zabezpieczeń TPM+Pin, TPM, Passphrase.
   3. Ochrona danych na budowanych dyskach twardych musi być realizowana przez silne szyfrowanie całej zawartości dysku/dysków oraz umożliwiać uwierzytelnianie użytkownika przed uruchomieniem startu systemu operacyjnego ze wsparciem metod silnego uwierzytelnienia.
   4. Ochrona danych przez szyfrowanie całej zawartości dysku oznacza, że szyfrowaniu podlagają wszystkie informacje zapisane na dysku twardym (łączenie z system operacyjnym, sterownikami, zainstalowanymi programami, danymi itp.).
   5. Funkcjonalność szyfrowania / deszyfrowania nie może być realizowana w oparciu o dodatkowego agenta na stacji roboczej, musi być integralnym rozwiązaniem oferowanego systemu.
   6. System musi umożliwiaż zdalne szyfrowanie / defszyrowanie partycji systemowych oraz prezentować bieżący postęp tego procesu.
   7. Proces szyfrowania odbywa się w sposób przezroczysty dla użytkownika komputera i może być realizowany w czasie jego pracy na komputerze. Szyfrowanie nie może być wyłączone przez użytkownika.
   8. Proces szyfrowania może być zatrzymany podczas hibernacji oraz wyłączenia systemu, ale jest kontynuowany po wzbudzeniu komputera / włączeniu.
   9. System musi umożliwiać szyfrowanie / deszyfrowanie komputerów w sieci lokalnej oraz poza NATem.

Załącznik A - Opis przedmiotu zamówienia zastępuje się **Załącznik A – ZMIANA - Opis przedmiotu zamówienia.**

W związku ze zmianą opisu przedmiotu zamówienia Zamawiający dokonuje zmiany terminu składania i otwarcia ofert:

**obecnie jest:**

**CZĘŚĆ XII**

**MIEJSCE ORAZ TERMIN SKŁADANIA I OTWARCIA OFERT**

Ofertę należy złożyć w Urzędzie Gminy Proszowice, 32-100 Proszowice, ul. 3 Maja 72, Biuro Obsługi Interesanta (Dziennik Podawczy, parter), **w terminie do dnia 15 stycznia 2021 r. do godz. 11.00**.

Oferty zostaną otwarte w Urzędzie Gminy Proszowice, 32-100 Proszowice, ul. 3 Maja 72, sala ślubów, **w dniu 15 stycznia 2021 o godz. 12.30**.

**po zmianie:**

**CZĘŚĆ XII otrzymuje brzmienie:**

**MIEJSCE ORAZ TERMIN SKŁADANIA I OTWARCIA OFERT**

Ofertę należy złożyć w Urzędzie Gminy Proszowice, 32-100 Proszowice, ul. 3 Maja 72, Biuro Obsługi Interesanta (Dziennik Podawczy, parter), **w terminie do dnia 20 stycznia 2021 r. do godz. 11.00**.

Oferty zostaną otwarte w Urzędzie Gminy Proszowice, 32-100 Proszowice, ul. 3 Maja 72, sala ślubów, **w dniu 20 stycznia 2021 o godz. 11.30**.

Burmistrz Gminy i Miasta Proszowice

Grzegorz Cichy