Podstrategia informatyzacji obszaru funkcjonalnego powiatu mikołowskiego

wraz z przygotowaniem Planu Operacyjnego na lata 2016-2025 w ramach projektu pod nazwą „J-ednolita S-trategia T-erytorialna = spójny obszar funkcjonalny powiatu mikołowskiego poprzez wzmocnienie mechanizmów efektywnej współpracy JST”

Załącznik A. Szczegółowa koncepcja rozwiązania w zakresie systemu bezpieczeństwa i ochrony danych dla wszystkich urzędów i jednostek organizacyjnych

Zamawiający:

Zarząd Powiatu Mikołowskiego

ul. Żwirki i Wigury 4a

43-190 Mikołów

Wykonawca:

Centrum Doradztwa w Informatyce i Zarządzaniu Sp. z o.o.

ul. Mogilska 25

31-542 Kraków

Kraków 2015

Spis treści

Załącznik A. Szczegółowa koncepcja rozwiązania w zakresie systemu bezpieczeństwa i ochrony danych dla wszystkich urzędów i jednostek organizacyjnych

1. Opracowanie dokumentacji oraz wdrożenie systemu SZBI

Warunki minimalne dla opracowania wzorcowej Dokumentacji Systemowej Bezpieczeństwa Informacji i Ochrony Danych do zgodności z normą PN ISO/IEC 27001:2014-12z uwzględnieniem Rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz.U. z 2004 r. Nr 100, poz. 1024) oraz Rozporządzenia Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (Dz.U. z 2012 r. Poz. 526), w tym opracowanie w minimum :

- Procedury audytu wewnętrznego Systemu Zarządzania Bezpieczeństwem Informacji;
- Procedury nadzoru nad dokumentacją Zamawiającego;
- Procedury i mierników badania efektywności Systemu Zarządzania Bezpieczeństwem Informacji;
- Struktury ról i odpowiedzialności w Systemie Zarządzania Bezpieczeństwem Informacji;
- Procedury okresowego przeglądu Systemu Zarządzania Bezpieczeństwem Informacji;
- Procedury audytu wewnętrznego;
- Procedury nadzoru nad Dokumentacją Systemową;
- Procedury działań korygujących i zapobiegawczych;
- Procedury nadawania, przeglądu i odbierania uprawnień do systemów i aplikacji;
- Procedury wykonywania i testowania kopii zapasowej;
- Procedury zabezpieczania przed szkodliwym oprogramowaniem;
- Procedury wykonywania i testowania Planów Ciągłości Działania wraz z opracowanymi pełnymi Planami Ciągłości Działania i Planami Odtworzeniowymi dla zidentyfikowanych procesów i systemów krytycznych z punktu widzenia bezpieczeństwa informacji Zamawiającego;
- Procedury i polityki oraz instrukcji zgodnych z wymaganiami prawnymi w obszarze ochrony danych osobowych - ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (tekst jednolity: Dz.U. z 2002 r. Nr 101, poz. 926 z późn. zm.);

- Procedury dostępu do pomieszczeń biurowych oraz pobierania, zdawania oraz przechowywania kluczy do pomieszczeń, budynków biurowych, technicznych;
- Procedury zarządzania incydentami bezpieczeństwa informacji;
- Deklaracji stosowania;
- Polityki Bezpieczeństwa Informacji.

2. Zakup osprzętu oraz konfiguracja i wdrożenie zabezpieczeń

Opis wymagań minimalnych

Nr	Wyposażenie
1.	Obudowa: RACK 1U.
2.	Procesor: Jeden procesor czterordzeniowy z obsługą instrukcji 64 bitowych umożliwiający osiągnięcie wyniku min. 6800 punktów w teście PassMark CPU Benchmarks dostępnym na stronie http://www.cpubenchmark.net/high_end_cpus.html. Procesor z obsługą wirtualizacji.
3.	Pamięć: min. 16GB dedykowane do pracy serwerowej.
4.	4 kieszenie HotSwap SATA3.
5.	1 dysk systemowy o poj. min. 1TB zamontowany w kieszeni HotSwap.
6.	3 dyski na dane o poj. min. 1TB zamontowane w kieszeniach HotSwap.
7.	Obsługa sieci: min. 2 karty sieciowe LAN RJ45 10/100/1000 Mb/s.
8.	Wsparcie KVM przez LAN.
9.	Panel przedni chroniący kluczem dostępu do dysków.
10.	Czujnik otwarcia obudowy.
11.	Zasilacz: min. 350W Gold certyfikat.
12.	System operacyjny: min. 64 bit.
13.	Komplet szyn montażowych w zestawie.
14.	Gwarancja: 2 lata gwarancji producenta.
15.	Dokumentacji w języku polskim.

Nr	Wyposażenie dodatkowe (Serwisowy Pendrive 8GB przechowujący konfigurację serwera oraz licencje)
1.	Szyfrowanie algorytmem min. AES256.
2.	Pendrive umożliwia pracę na ograniczonych uprawnieniach użytkownika.
3.	Możliwość blokady zapisu na serwisowym pendrive dla klientów Windows.
4.	Możliwość przypisania litery dysku, który zostanie odszyfrowany.
5.	Przechowywanie i przywrócenie fabrycznych ustawień urządzenia.
6.	Możliwość tworzenia backupu i ustawień systemu serwera.
7.	Tryb diagnostyczny pozwalający: • diagnostykę dysków twardych; • możliwość zmiany parametrów dysków min. pozwalając na obniżenie wydajności

	kosztem zwiększenia trwałości; • dostęp do uszkodzonych dysków; • wykonanie kopii danych w trybie binarnym; • dostęp do narzędzi partycjonowania.
8.	Przechowywanie kluczy licencji.
9.	Narzędzia diagnostyczne dla kontrolera Domeny pozwalające na (naprawę bazy danych Domeny, dostęp do partycji kontrolera domeny, przywrócenie ustawień początkowych).

Nr	**Oprogramowanie serwera (Zarządzanie systemem i konfiguracją przez przeglądarkę WEB)**
1.	Interfejs obsługi serwera musi być realizowany przez najnowszą przeglądarkę internetową i być w standardzie Windows METRO.
2.	System powinien przed zalogowaniem do panelu zarządzającego informować w czasie rzeczywistym administratora o obciążeniu: całego systemu, procesora, pamięci oraz interfejsu sieciowego na dynamicznych wykresach. Wskazując myszką dane na wykresie powinny pokazywać wartość obciążenia. Informacje o obciążeniu całego systemu, procesora, pamięci oraz interfejsu sieciowego powinny być archiwizowane w serwerze i dostępne przez system raportujący dla okresów: godzinowy, dzienny, tygodniowy i miesięczny.
3.	Menu dostępu do poszczególnych funkcji serwera powinno mieć możliwość konfigurowania położenia oraz kolorów.
4.	Serwer musi umożliwiać realizowanie usług (FTP, FTP z opcją szyfrowania SSL/TLS, TFTP, NFS, SSH).
5.	Musi posiadać system antywirusowy.
6.	Możliwość zarządzania serwerem poprzez protokół SNMP w wersji 1/2/3.
7.	Musi umożliwiać dostęp administratorów przez przeglądarkę WEB.
8.	Musi umożliwiać obsługę 4 dysków SATA III.
9.	Umożliwiać szyfrowany dostęp SSL/TLS dla serwera FTP.
10.	Blokowanie dostępu użytkownikom po adresie IP, protokole sieciowym, porcie komunikacyjnym, adresie MAC za pomocą przeglądarki WEB.
11.	Integracja z Microsoft Active Directory w zakresie dostępu użytkowników do zasobów.
12.	Możliwość pracy z systemami plików ext3, ext4, xfs, jfs.
13.	Wbudowany terminarz zadań (możliwość wywołania cyklicznych zadań) zarządzany przez przeglądarkę WEB: • tworzenie zadań dla ustawień: minut, godzin, dni w miesiącu, miesiąc, dni w tygodniu, • tworzenie zadań z poświadczeniami wybranego użytkownikami, • powiadomienie na adres email o wyniku wykonanego zadania.
14.	Wbudowany firewall i ustalania routingu przez przeglądarkę WEB.
15.	Możliwość zmiany konfiguracji usługi FTP: • zmiany portu, na którym działa usługa (domyślnie jest to port 21), • określenie maksymalnych ilości podłączonych klientów, • określenie maksymalnej ilości połączeń na jeden adres IP,

	• określenie maksymalnej ilości prób logowania, • możliwość ustawienia wiadomości powitalnej dla klientów usługi, • możliwości użycia ograniczeń przepustowości pobierania i wysyłania danych, • możliwość ustawienia zakresu portów podczas pasywnego FTP, • możliwość włączenia protokołu jednostkowego - identyfikacji (RFC1413), • możliwość przypisania certyfikatu SSL/TLS.
16.	Opcje usługi SSH: • ustawienie portu dla usługi SSH, • zezwalaj na logowanie root-a – włączenie tej opcji powoduje, że możemy zalogować się na serwer jako administrator z pełnią praw, • tunelowanie połączeń TCP przez SSH.
17.	Obiekty i-SCSI: • tworzenie obiektów LUN, • szyfrowanie nagłówka, • uporządkowane dane, • max ilość połączeń w ciągu sesji, • max ilość sesji.
18.	Tworzenie RAID 0,1,10,5,6,
19.	System musi pokazywać w przeglądarce WEB numery seryjne dysków oraz ich temperaturę użytkowania.
20.	System musi umożliwiać tworzenie i zarządzanie logicznymi woluminami oraz dynamiczne alokowanie przestrzeni.
21.	Przed zalogowaniem administratora do interfejsu serwera WEB, można bez autoryzacji odczytywać parametry obciążenia serwera pokazywane na dynamicznych wykresach w przeglądarce WEB.
22.	Autoryzacja do interfejsu WEB musi być realizowana przy pomocy protokołu SSL.
23.	System musi umożliwiać generowanie certyfikatów SSL przez przeglądarkę WEB.
24.	System powinien posiadać magazyn przechowywania i zarządzania certyfikatami SSL zarządzany przez przeglądarkę WEB.
25.	System powinien posiadać możliwość importowania zewnętrznych certyfikatów SSL przez przeglądarkę WEB.
26.	System powinien posiadać logi z następujących usług odczytywane przez przeglądarkę WEB: • Antywirus, • FTP, • Uwierzytelnianie.

Nr	Obsługa domeny
1.	Zarządzanie do min. 50 użytkowników, grup oraz komputerów, urządzeń.
2.	Tworzenie i zarządzanie domenami, drzewami i lasami.
3.	Integracja z podstawowymi i zapasowymi kontrolerami domeny.
4.	Zarządzanie polisami GPO.

5.	Wsparcie dla pojedynczego logowania.
6.	Obsługa profili użytkowników oraz profili mobilnych.
7.	Obsługa do 50 jednoczesnych podłączeń do serwera domen.
8.	Zarządzanie użytkownikami, grupami, komputerami podpiętymi do kontrolera domenowego przez przeglądarkę WEB.
9.	Możliwość tworzenia użytkowników i grup w kontrolerze domeny przez przeglądarkę WEB.
10.	Nadawanie haseł dla użytkowników w kontrolerze domeny przez przeglądarkę WEB.
11.	Wyszukiwanie po nazwie użytkownika, grupy i komputera przez przeglądarkę WEB.
12.	Lista użytkowników, którym wygasła ważność konta dostępna w przeglądarce WEB.
13.	Lista zablokowanych kont w kontrolerze domeny dostępna w przeglądarce WEB.
14.	Wszystkie operacje zakładania i modyfikacji oraz usuwania kont, grup, komputerów w kontrolerze domenowym raportowane w centralnym repozytorium systemowych zdarzeń dostępnym przez przeglądarkę WEB.
15.	Współpraca z klientami Windows 2000, XP, Vista,7,8,8.1 w wersji professional.

Nr	**Oprogramowanie**
1.	Działające w systemie Windows Vista,7,8,8.1 w wersji 32 i 64 bity w wersji professional z licencją bezterminową umożliwiającą przenoszenie do 50 użytkowników lokalnych do serwera domenowego, które realizuje: • Automatyczne przenoszenie profili i ustawień użytkownika z konta lokalnego do konta domenowego, • Automatyczne przeniesienie dokumentów użytkownika z konta lokalnego do konta domenowego i nadanie odpowiednich uprawnień ACL, • Automatyczne przenoszenie uprawnień plikowych i rejestru z konta lokalnego do konta domenowego, • Automatyczne przeniesienie lokalnej skrzynki pocztowej Microsoft Outlook i Thunderbird z domyślnej lokalizacji w koncie lokalnym do konta domenowego, • Możliwość pozostawienia ustawień konta lokalnego użytkownika po migracji do konta domenowego.

Nr	Obsługa wirtualizacji
1.	Obsługa wirtualizacji dowolnych systemów operacyjnych.
2.	Obsługa minimum cztero-rdzeniowego procesora.
3.	Obsługa minimum 8GB RAM-u.
4.	Obsługa vmware VMDK.
5.	Obsługa minimum 5 instancji środowisk wirtualnych.
6.	Zapis stanu maszyny wirtualnej tzw. Snapshot.
7.	Kopia stanu maszyny wirtualnej.
8.	Dwustronny schowek na dane.
9.	Możliwość automatycznej zmiany rozdzielczości ekranu w systemie gościa.
10.	Obsługa współdzielonych folderów i kontenerów danych tzw. Shared Storage.

11.	Obsługa RDP.
12.	Emulacja wielu urządzeń np. kart sieciowych, kontrolerów SAS.
13.	Obsługa akceleracji 3d.
14.	Wirtualizacja 64 bitowych systemów na procesorach 32 bitowych.
15.	Dynamiczna alokacji pamięci na kontener danych.
16.	Obsługa wirtualizacji sprzętowej Intel VT-x oraz AMD-V.
17.	Obsługa SMP dla procesorów Intel VT oraz AMD-V.
18.	Współpraca z kontrolerami SATA, SCSI.
19.	Tryby pracy sieciowej min NAT, tunel UD, Bridge oraz wielu interfejsów sieci.
20.	Wsparcie dla środowisk Windows 32 oraz 64 bity w wersjach desktop oraz serwer min (Windows 2000,XP,2003,2008,vista,7,8), Linux 32 oraz 64 bity, MacOS.
21.	Zarządzanie poprzez przeglądarkę WEB.
22.	Archiwizacja uruchomionych maszyn wirtualnych.

3. Zakup licencji systemu monitoringu

Opis licencji oprogramowania do elektronicznego systemu/portalu monitoringu sieci, infrastruktury o minimalnej funkcjonalności z zakresu bezpieczeństwa infrastruktury i nadzoru ICT organizacji indywidualnych stanowisk pracy(stacji roboczych) według opisanej poniżej funkcjonalności :

1. **Wymagania ogólne**

- System musi zawierać 3 warstwową architekturę (agent, serwer aplikacji, baza danych).
- Agent aplikacji (oprogramowanie instalowane na komputerze klienta komunikujące się, dokonujące autoryzacji i optymalizujące połączenia wyłącznie poprzez oprogramowanie pośredniczące tzw. serwera aplikacji. Oprogramowanie Agenta nie może instalować, zmieniać ustawień, aktualizować oraz w jakikolwiek bezpośredni sposób komunikować się z bazą danych).
- Serwer aplikacji (zainstalowane oprogramowanie na komputerze serwera, pracującego w sposób ciągły, zbierające informację od zainstalowanych agentów i zarządzające nimi. Oprogramowanie serwera wysyła raporty na email, dokonuje aktualizacji agentów, odpowiada za proces licencjonowania systemu, dokonuje zapisywania i odczytywania informacji z bazy danych. Serwer aplikacji posiada wewnętrzny terminarz pozwalający na powiadamianie i wykonywanie ustalonych zadań zgodnie z ustalonym okresem, nawet gdy agenci są wyłączeni lub niedostępni).
- Baza danych (oprogramowanie współpracujące z serwerem aplikacji, przechowujące ustawienia oraz informacje z agentów. Baza danych musi być w pełni funkcjonalna, nie może to być wersja express, standard. Baza danych musi zawierać licencję na 1 połączenie, pozwalające serwerowi aplikacji na współpracę. Baza danych nie może komunikować się z serwerem aplikacji poprzez protokół TCP/IP. Nie może również otwierać innych gniazd sieciowych pozwalających na dostęp z zewnątrz. Baza danych musi być kompatybilna z zainstalowanymi bazami danych).

- Konsola (oprogramowanie łączące się z serwerem aplikacji w sposób intuicyjny pozwalający administratorowi na zarządzanie systemem oraz komputerami).
- System musi być kompatybilny z systemami Windows 2000/XP/2003/Vista/2008/7/8 w wersjach 32 oraz 64 bit oraz ich wersjami serwerowymi.
- Licencja umożliwia instalację dowolnej liczby konsol i serwerów.
- Licencja nie może korzystać ze sprzętowych kluczy HASP ani zajmować wolnych portów USB, LPT.
- Baza danych stanowi integralną część systemu do której dostęp ma wyłącznie dedykowany i oddzielny proces serwera aplikacji.
- Baza danych musi być całkowicie bezpłatna o pełnych możliwościach, nie w wersji express ani standard.
- Do instalacji serwera centralnej administracji nie jest wymagane zainstalowanie żadnych dodatkowych baz typu MSDE lub MS SQL.
- Do instalacji serwera centralnej administracji nie jest wymagane zainstalowanie dodatkowych aplikacji, takich jak Internet Information Service (IIS) czy Apache.
- System musi posiadać możliwość zdalnej instalacji agentów oprogramowania bez zainstalowanej usługi Active Directory.

2. Funkcje Agenta aplikacji

- Agent musi pracować jako usługa systemowa.
- Agent aplikacji musi pracować na ograniczonych prawach użytkownika.
- Agent musi pracować w sytuacjach gdy serwer aplikacji jest chwilowo niedostępny.
- Agent musi posiadać funkcje uniemożliwiające zabicie procesu agenta.
- Agent musi posiadać funkcje uniemożliwiające odinstalowanie agenta pytając o hasło.
- Interfejs agenta musi pozwalać na konfigurację mechanizmu blokady USB, procesów, urządzeń w momencie gdy agent nie jest podłączony do sieci firmowej.
- Zmiana (adresu IP, MAC, Nazwa komputera) na komputerze gdzie zainstalowany jest agent nie może powodować utraty informacji, ustawień, reguł dla danego komputera.
- Komunikacja Agenta z serwerem aplikacji powinna być w trybie natychmiastowym oraz co określoną ilość sekund.

3. Funkcje serwera aplikacji

- Serwer aplikacji musi pracować jako usługa systemowa.

- Serwer aplikacji musi zawierać terminarz pozwalający na wykonywanie zaplanowanych zadań, wysyłający określone raporty na email, nawet w chwili gdy komputery gdzie agent jest zainstalowany nie są dostępne.
- Serwer aplikacji musi mieć możliwość pobrania aktualnej bazy danych poprawek systemu Windows. Baza informacji o aktualizacjach Windows musi zawierać nazwę poprawki oraz wymagania jakie dana poprawka musi spełnić aby być zainstalowana na komputerze.
- Serwer musi mieć możliwość zdalnej aktualizacji oraz instalacji agenta aplikacji bez zainstalowanej usługi Active Directory. Baza poprawek powinna zawierać informacje o poprawkach krytycznych, bezpieczeństwa, service pack.
- Zewnętrzne dodatkowe narzędzia służące do poprawnej konserwacji bazy danych, archiwizacji i optymalizacji powinny być zawarte w pakiecie. Narzędzia służące do konserwacji bazy danych muszą współpracować z terminarzem zadań Windows wykorzystując jego możliwości określenia terminu wykonania zadania, konta użytkownika.
- Terminarz zadań powinien pozwalać na określenie daty, godziny i minuty uruchomienia zadania, częstotliwości uruchamiania zadań oraz okresu daty i czasu w jakich dane zadanie ma być uruchamiane. Zdefiniowane zadanie powinno mieć status wykonania (tzn. uruchomiono, nie uruchomiono, zakończono wykonywanie). Zadania muszą być zdefiniowane dla (sprawdzenia poprawek, instalacji poprawek, eksportu oprogramowania, eksportu historii oprogramowania, audytu plikowego oprogramowania, eksportu sprzętu, eksportu procesów, eksportu rejestru systemowego, eksportu listy katalogów, eksportu zdarzeń systemowych, eksportu usług, wyłączenia komputera, restartu komputera).

4. Funkcje konsoli

- Konsola powinna mieć możliwość określenia serwera aplikacji do którego chce się podłączyć.
- Konsola powinna mieć możliwość określenia drzewiastej struktury zarządzania tzn. grupa komputerów jako kontener zawierający agentów.
- Konsola musi pozwalać na definiowanie ustawień dla poszczególnych agentów, grup agentów z możliwością automatycznego dziedziczenia tych ustawień. W chwili przenoszenia agenta pomiędzy grupami ustawienia powinny się dziedziczyć z grupy docelowej. Konfigurowanie agentów musi działać nawet w chwili gdy komputery pracujące pod kontrolą agentów nie są dostępne.
- Konsola powinna mieć spójny interfejs pozwalający administratorowi na drukowanie, multi sortowanie, grupowanie po wybranej kolumnie, stosowanie filtrów wyświetlania w oparciu o wyrażenia regularne, zapisywanie w postaci raportu informacji z możliwością szybkiego ich wczytania, eksportowanie do html, xml, xlsx, docx.
- Wydruk informacji z konsoli powinien pozwalać na umieszczanie dodatkowych informacji na drukowanych elementach w stopce i nagłówku pozwalając na dodanie dodatkowych grafik.

Dodatkowo wybrany wydruk powinien mieć możliwość skierowania informacji do Worda i Excela.

5. Zarządzanie systemowym dziennikiem zdarzeń

- Oprogramowanie musi archiwizować w centralnej bazie systemu dzienniki (aplikacji, systemu i bezpieczeństwa) dla wybranego komputera, nawet w przypadku gdy określony komputer nie jest dostępny w sieci firmowej.
- Dane z dziennika zdarzeń powinny być zapisywane według wbudowanego terminarza zadań.

6. Zarządzanie aktualizacjami dla systemu Windows

- Oprogramowanie musi automatycznie według terminarza dokonywać sprawdzenia brakujących i nieaktualnych poprawek na wybranych komputerach, wraz z możliwością natychmiastowej ich instalacji.
- Oprogramowanie musi samo dbać o poprawną i ciągłą instalację kilku poprawek, jednocześnie service packów, aktualizacji wymagających uruchomienia komputera.
- Oprogramowanie musi posiadać możliwość odinstalowania lub nadpisania określonych aktualizacji.
- Oprogramowanie musi informować administratora o właściwościach danej aktualizacji takich jak: (Tytuł poprawki, opis poprawki, ważność poprawki, kategoria, język poprawki, czy administrator dokonał ręcznego wskazania aktualizacji do instalacji, data publikacji, adres www skąd pobrano aktualizację, adres www biuletynu bezpieczeństwa, adres www z dodatkowymi informacjami technicznymi, czy aktualizacja jest w wersji beta, czy wymaga zaakceptowania dołączonej licencji itp.).
- Oprogramowanie musi pozwalać na całkowicie cichą instalację poprawki nie wymagając od użytkownika ani administratora żadnego potwierdzenia czynności np. dotyczących licencji.
- Oprogramowanie musi samo decydować czy po zainstalowaniu poprawki wymagane jest uruchomienie komputera czy nie. Niedopuszczalne jest resetowanie komputera po zainstalowaniu aktualizacji w chwili wykonywania operacji przez użytkownika.
- Oprogramowanie automatycznie powinno sprawdzać czy jest dostępna wolna przestrzeń dyskowa na instalację poprawek.
- Oprogramowanie do poprawnego informowania o zainstalowanych poprawkach oraz ich instalacji nie może polegać na informacjach dostępnych w rejestrze systemowym oraz nie może wymagać od administratora pobranej aktualizacji na komputer lokalny. W celu określenia brakujących i pasujących poprawek system musi odczytywać zależności pomiędzy wersjami plików aktualizacji już zainstalowanych np. Windows Media Player, zainstalowany Service Pack.

- Oprogramowanie samo musi decydować czy dana poprawka pasuje do wybranego systemu operacyjnego i zainstalowanych innych poprawek i service packów oraz informować o tym.
- Oprogramowanie musi mieć możliwość jednoczesnej instalacji danej poprawki na wielu komputerach.
- Oprogramowanie nie może wymagać zainstalowanej usługi Active Directory ani wersji serwer systemu operacyjnego.
- System musi mieć możliwość instalacji poprawek na ograniczonym koncie użytkownika.

7. Zarządzanie blokadą procesów, urządzeń usb, cd-rom

- Oprogramowanie musi mieć możliwość blokowania i dopuszczania Procesów, urządzeń usb, cd-rom w chwili niedostępności serwera aplikacji.
- Blokada urządzeń usb musi działać na szyfrowanych pamięciach usb oraz współpracować z hubami usb.
- Blokowanie pamięci usb nie może powodować blokowania całego portu usb, uniemożliwiając tym samym blokowanie innych urządzeń na tym porcie takich jak np. mysz, drukarka itp.
- Weryfikacja danej pamięci usb musi być dokonywana w chwili wpinania do portu (według takich reguł jak etykieta pamięci, numer seryjny urządzenia, dostępny klucz znajdujący się na pamięci)
- Blokada pamięci usb nie może modyfikować ustawień rejestru klucza:
- HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\StorageDevicePolicies, tak aby użytkownik nie mógł dokonywać samodzielnych zmian w rejestrze systemowym powodując destabilizację działania.
- Blokowanie urządzeń usb i cd-rom powinno działać na systemach starszych niż Windows XP Service Pack 2.
- Blokowanie oraz zezwalanie urządzeń usb musi działać w przypadku gdy jednocześnie pracuje kilka pamięci flash podpiętych do kilku portów.
- Kontrola procesów powinna być definiowana przynajmniej dla atrybutów (nazwa procesu, ścieżka, rodzaj dysku gdzie uruchamiany jest proces, producent, suma crc, rozmiar).
- System powinien umożliwiać blokadę wybranych urządzeń dostępnych poprzez menedżer urządzeń np. kartę sieciową.
- Oprogramowanie musi blokować/dopuszczać wybrane konkretne płyty cd-rom, dvd rom.
- Konfiguracja dostępu do urządzeń oraz procesów powinna być zorganizowania w sposób pozwalający na definiowanie polityki bezpieczeństwa wszystko blokuj i dopuszczaj tylko zdefiniowane oraz polityki wszystko dopuszczaj i zablokuj tylko wybrane dla parametrów takich jak np. (nazwa komputera, zalogowany użytkownik, nazwa procesu lub pamięci wymiennej, suma crcitp).

- Oprogramowanie powinno pozwalać na tworzenie własnego autoryzowanego magazynu nośników zewnętrznych.
- System powinien zbierać Informacje o modyfikowanych plikach na urządzeniach
- System powinien umożliwiać raportowanie uruchamianych procesów, pamięci usb i cdrom, wraz z informacją o komputerze gdzie wykorzystano niedozwolony proces czy pamięć usb.

8. Zdalny pulpit

- Zdalny pulpit powinien być integralną częścią systemu i posiadać funkcję zdalnego menedżera plików.
- Administrator musi kontrolować zdalny komputer nie powodując wylogowywania użytkownika. Wszystkie operacje powinny być widoczne przez użytkownika.
- Administrator może wykonywać działania na odległym komputerze z uprawnieniami administratora.
- Zdalny pulpit powinien mieć możliwość konfiguracji kompresji, rozdzielczości.
- Zdalny pulpit powinien umożliwiać podgląd ekranu zdalnego komputera bez przejęcia kontroli.

9. Zdalna linia poleceń

- Administrator powinien móc wykonywać skrypty batch w trybie administratora.
- System musi zapisywać wszystkie polecenia jakie administrator wykonywał.
- Oprogramowanie musi umieć wykonywać interaktywne polecenia, wymagające potwierdzenia operacji takie jak np. "format d:"

10. Funkcjonalność zarządzania instalacją i aktualizacją oprogramowania

- System musi pozwalać na instalację cichą również programów skompresowanych i w razie potrzeby dokonywać restartu komputera.
- Przed instalacją oprogramowania system musi zarchiwizować starszą wersję instalowanego programu i umożliwiać w razie potrzeby przywrócenie starszej wersji.
- Instalacja oprogramowania powinna pozwalać na tzw. instalację różnicową pozwalając instalować tylko pliki o nowszej wersji dla docelowej aplikacji.
- Zainstalowane aplikacje mogą wymagać odinstalowania i system zarządzający instalacją musi to umożliwiać.
- System musi mieć możliwość instalowania jednocześnie kilku aplikacji zdefiniowanych w instalatorze dla wielu komputerów.

- System musi umieć stworzyć instalator zawierający kilka aplikacji tzw. metodą snapshot tzn. w sposób pozwalający administratorowi stworzyć wzorcową instalację oprogramowania i wykazanie różnicy zmian w systemie operacyjnym, jakie nastąpiły pomiędzy zainstalowaną, a nie zainstalowaną aplikacją. Stworzony instalator po uruchomieniu na docelowym komputerze musi pozwalać na instalację całkowicie cichą, tak aby użytkownik widział tylko zainstalowaną aplikację, a nie proces instalacji.
- Tworzony instalator zawierający aplikacje powinien pozwalać na instalację dla wybranego użytkownika docelowego komputera.
- System musi raportować o postępie i błędach w instalacji oprogramowania.
- Dla zainstalowania aplikacji w odległym komputerze, system musi pozwalać na instalację aplikacji w formacie skompresowanym exe, msi oraz w formacie stworzonego instalatora dla określonego użytkownika nawet jeżeli zalogowany zdalny użytkownik jest inny niż wskazany w paczce instalacyjnej.
- Program musi tworzyć instalator oprogramowania w formacie msi.
- System musi pozwalać na stworzenie instalatora zawierającego możliwość odinstalowania aplikacji oraz zmiany w konfiguracji już zainstalowanego programu.
- System musi umożliwiać uruchamianie dowolnego zainstalowanego już oprogramowania wymagającego praw administratora w przypadku gdy zalogowany jest użytkownik na ograniczonych prawach. System powinien w tym celu posiadać specjalny pulpit pozwalając użytkownikom na uruchamianie takich programów jednym kliknięciem.
- System powinien tworzyć skompresowaną listę plików które mogą być tworzone i przesyłane jako wzorcowe dane i dokumenty dla użytkowników.

11. Zdalne zarządzanie kontami użytkownika, uprawnieniami do plików i katalogów do rejestru

- Zdalne zarządzanie kontami użytkowników, uprawnieniami do plików, katalogów, rejestru oraz inspekcja tych obiektów musi być możliwa nawet w przypadku gdy zdalny komputer nie jest dostępny w sieci firmowej. W momencie podpięcia komputera do firmowej sieci informacje o kontach, uprawnienia oraz inspekcja powinny być zsynchronizowane i zastosowane.
- Zarządzanie użytkownikami powinno obejmować min takie operacje jak tworzenie użytkownika i grupy ,ustalanie hasła oraz przynależności do określonych grup.
- Zarządzanie uprawnieniami do plików i katalogów musi być zgodne z formatem ACL i współpracować z istniejącymi już ustawieniami ACL na komputerach.
- Stosowanie inspekcji komputerów również musi pozwalać na zmianę systemowych ustawień inspekcji ACL na obiektach plików, katalogów i rejestru.
- Zdalne zarządzanie rejestrem systemowym.

12. Zarządzanie usługami Windows

- Konfiguracja usług musi dotyczyć komputerów podpiętych do sieci firmowej oraz chwilowo niedostępnych.
- Administrator powinien mieć przynajmniej możliwość określania takich parametrów usług jak: (Nazwa usługi, opis, ścieżka, konto na którym dana usługa będzie uruchamiana, tryb uruchomienia usługi: Boot, system, Ręczne i automatyczne).
- System powinien pozwalać tak skonfigurować usługę, że pomimo gdy ona będzie generowała błąd podczas startu nastąpi jej uruchomienie.

13. Blokowanie stron internetowych

- Program musi mieć możliwość sprawdzenia czy dana strona nie jest fałszywa poprzez mechanizm Antyphisingu.
- Blokowanie stron internetowych nie może polegać na zabiciu procesu przeglądarki. System powinien poinformować użytkownika w postaci strony internetowej, która może być stworzona przez administratora jako szablon.
- Blokowanie stron internetowych powinno dotyczyć takich przeglądarek jak Internet Explorer, Microsoft Edge, Firefox, Chrome, Safari, Opera.
- System musi blokować strony internetowe zawierające reklamy, wyskakujące okna, skrypty java, banery, obiekty flash, pliki cookies.
- System powinien zabezpieczać przeglądarki przed przepełnieniem bufora podczas przetwarzania plików jpeg.
- Blokowanie lub dopuszczanie stron internetowych powinno być oparte na definiowanych regułach zgodnie z zasadą wszystko blokuj i dopuszczaj tylko określone oraz odwrotnie. Konfigurowanie stron www powinno umożliwiać stosowanie znaków zastępowania takich jak *,? itp. Reguły powinny pozwalać dopuszczać lub blokować również strony będące pod domenami stron głównych np. w stosunku do strony www.onet.pl
- Administrator powinien mieć możliwość zablokowania plików które użytkownik może pobierać z Internetu min plików exe, vb, bat, msi, tar itp.
- Informacje o zablokowanych i dopuszczonych stronach powinny być dostępne administratorowi w postaci logów.

14. Monitorowanie stron internetowych oraz aplikacji

- Monitorowanie stron internetowych powinno dotyczyć takich przeglądarek jak Internet Explorer, Microsoft Edge, Firefox, Chrome, Opera, Safari.
- Funkcjonalność monitorowania stron internetowych musi działać niezależnie od historii odwiedzanych stron zapisywanych przez przeglądarkę internetową.

- W przypadku gdy użytkownik przegląda jednocześnie wiele stron internetowych na poszczególnych zakładkach przeglądarki, system musi zliczać przebywanie na każdej zakładce, ale tylko w momencie gdy dana zakładka jest aktywna.
- Odwiedzane strony internetowe powinny być zapisywane w systemie z dokładnością do 5 sekund.
- Powinny być gotowe zdefiniowane raporty dzienne, tygodniowe, miesięczne.
- Raporty powinny zawierać takie informacje jak (nazwa komputera, nazwa strony www lub programu, data i czas otwarcia strony lub programu, data i czas zamknięcia strony lub programu, czas pracy, użyta przeglądarka, zalogowany użytkownik).
- System musi mieć możliwość cyklicznego co określoną liczbę sekund pobierania zrzutów ekranu z aktualnie używanej aplikacji.
- System nie może instalować żadnych sterowników, keylogerów, programów nadzorujących pracę klawiatury lub myszki, tak aby programy antywirusowe nie traktowały tego jako niezweryfikowanego zagrożenia.
- System powinien informować o okresach bezczynności komputera.
- System musi umożliwiać nadzorowanie oraz informowanie o plikach kopiowanych, przenoszonych i modyfikowanych niezależnie od używanego menedżera plików, czy powłoki systemowej oraz używanego systemu operacyjnego. W szczególności system musi kontrolować systemy 64 bitowe oraz linie poleceń cmd.

15. Inwentaryzacja oprogramowania, sprzętu, procesów i licencji

- Inwentaryzacja musi mieć moduł odpowiedzialny za wykrywanie oprogramowania i sprzętu oraz moduł pozwalający na przyjęcia na majątek firmy obiektów, które nie mogą być automatycznie wykryte np. biurko, telefon, kabel UTP lub dowolny składnik będący na wyposażeniu działu IT.
- Proces audytowania sprzętu oaz oprogramowania musi składać się z 2 etapów:
    - Pierwszy etap zbieranie informacji sprzętowo programowej i zapis do systemu.
    - Drugi etap przyjęcie na majątek IT tylko takiego oprogramowania lub sprzętu, który jest istotny z punktu widzenia pracy działu IT np. licencjonowane oprogramowanie).
- Proces audytu programów (powinien wyciągać takie informacje jak Nazwa Programu, nazwa deinstalatora, wersja, producent, opis, adres www z informacjami o aplikacji, data instalacji, źródło instalacji np. CD-ROM, docelowa instalacja programu, język itp.).
- Dodatkowo program powinien zapisywać informacje o programach będących na pulpicie komputera oraz w Menu programy.
- System musi pozwalać przeskanować komputer i pobrać informacje dotyczące instalacji i odinstalowania aplikacji oraz innych znaczących zmian w konfiguracji komputera.

- Dodatkowo oprócz ewidencji oprogramowania system musi mieć możliwość ewidencji dowolnych plików, jakie mogą znajdywać się na komputerach. (W szczególności powinien zapisać informacje takie jak Ścieżka pliku, nazwa, ścieżka archiwum jeżeli dany plik znajduje się wewnątrz archiwum spakowanego, nazwa archiwum ,rozmiar pliku, crc pliku, czas użytkowania pliku, czas utworzenia pliku, wersja pliku.)
- Oprogramowanie powinno również odczytywać Prawa autorskie pliku.
- Audyt plikowy musi umożliwiać wyciągnięcie informacji o plikach będących w archiwum takim jak (zoo, cab, arj, rar, zip, tar, lhz, arc, ace).
- Audyt plikowy powinien mieć możliwość określania katalogów jakie będą podlegały skanowaniu oraz katalogów będących jako wykluczenie.
- Audyt plikowy powinien określać rozszerzenia plików które będą brane tylko pod uwagę np. tylko pliki "jpg".
- Audyt plikowy, oprogramowania, sprzętu powinien być wykonywany według terminarza wbudowanego, w chwili gdy komputer ma włączony wygaszacz ekranu lub natychmiast na żądanie administratora.
- Administrator powinien otrzymać informację o wykonanych zadaniach poprzez dziennik zdarzeń, email, informację w pliku xml, oraz dodatkowy program zewnętrzny który byłby uruchamiany.
- Wyniki przeprowadzonego audytu plikowego, oprogramowania oraz sprzętu powinny być wysyłane na email, do konkretnego katalogu na zdalnym serwerze oraz na serwer ftp.
- Audyt sprzętu powinien odczytywać informacje takie jak:
    - Informacje komputera (Model, Producent, nr seryjny, system operacyjny, wersja, product id, product key).
    - Informacje o obudowie (np. czy obudowa jest typu laptop, desktop, serwer itp.).
    - Informacje o płycie głównej (Producent, wersja, nr seryjny, assettag).
    - Informacja o pamięci operacyjnej z podziałem na sloty zajęte oraz wolne. Informacja o numerze seryjnym pamięci.
    - Informacja o procesorze (częstotliwość, cache, model, NR seryjny).
    - Informacja o karcie graficznej(Producent, rodzaj tzn. czy zintegrowana czy nie, zainstalowana pamięć, data sterownika oraz wersja).
    - Informacja o Monitorze (Producent, rodzaj, rozdzielczość, numer seryjny).
    - Urządzenia pamięci takie jak nagrywarki DVD oraz CD.
    - Informacja o dyskach twardych (interfejs tzn. np. IDE, SCSI, rozmiar fizyczny dysku, numer seryjny).

  - Informacja o partycjach takie jak (numer seryjny, wolny i całkowity rozmiar, system plików, kompresja).
  - Informacja o fizycznej karcie sieciowej oraz konfiguracja sieci (Adres bramy, adres IP, adres MAC, adres serwera DHCP, adres serwera DNS).
  - Informacje o dacie produkcji komputera.
  - Informacje o urządzeniach peryferyjnych takich jak Drukarki.
  - Informacje o posiadaniu baterii.
  - Informacje o zainstalowanym Streamerze.
  - Informacje o zainstalowanych slotach pamięci takich jak pci, agp.
  - Informacje o aktywacji oraz instalacji systemu operacyjne.
- Ewidencja oprogramowania powinna informować o uruchomionych programach i użytkowniku korzystającego z programu.
- Program musi odczytywać numery seryjne, klucze licencyjne, produkt id, użytkowniku który licencjonował aplikację, typ licencji np. oem dla systemu operacyjnego Windows 2000, XP, 2003, 2008, vista, 7,8 w wersjach 32 i 64 bity oraz dla Microsoft Office 2000, XP, 2003, 2007, 2010 w wersjach 32 i 64 bity.
- Program musi dodatkowo odczytywać klucze licencyjne i numery seryjne metodą heurystyczną dla innych programów min. dla nero.
- Ewidencja oprogramowania powinna zawierać listę sterowników zainstalowanych na komputerze i odczytywać następujące parametry sterownika (Nazwa urządzenia, grupa urządzenia, producent, data i wersja sterownika, plik sterownika, Acpi).
- Audyt plikowy powinien być uruchamiany i dokonywać odczytu plików w chwili podpięcia pamięci USB lub płyty CD.
- Administrator powinien mieć zdefiniowane następujące raporty:
  - audyt plików z licencją freeware,
  - audyt plików mp3,
  - audyt plików pogrupowany wobec nazwy pliku,
  - audyt plików pogrupowany wobec producenta,
  - komputery typu laptop,
  - lista oprogramowanie gdzie dla różnych komputerów są te same klucze licencyjne.
- Oprócz zdefiniowanych raportów system musi pozwalać na tworzenie i zapisywanie własnych raportów w oparciu o wszystkie pola sprzętu i oprogramowania, które system odczytuje z komputerów. W szczególności system powinien pozwalać na tworzenie filtrów "właściwość pola=wartość pola". Administrator tworząc własny raport powinien móc opisać go polami

(nazwa raportu, opis, data utworzenia, autor, wersja raportu oraz czy dany raport powinien być dostępny w menu głównym, wraz ze standardowymi raportami).

- Dowolny standardowy lub stworzony przez administratora raport powinien pozwalać na wykazanie różnic pomiędzy dwoma dowolnymi datami przeprowadzonego skanowania.
- Dowolny standardowy lub stworzony przez administratora raport powinien zapisywać do systemu tylko zmiany jakie dokonywane były podczas ostatniego przeprowadzonego skanowania. Takie historyczne raporty powinny pozwalać administratorowi określać zakres dat (od / do określonej daty).
- Standardowe lub stworzone raporty powinny być wysyłane na email zgodnie z terminarzem np. raporty(o nowo uruchomionych procesach, nowych plikach, zmianie konfiguracji sprzętowej np. wymianie pamięci RAM, nowo zainstalowanych programach itp.).
- Dane audytu plikowego, oprogramowania oraz sprzętu powinny mieć możliwość zaimportowania z komputerów, które nie są dostępne w sieci firmowej.
- Audyt oprogramowania, sprzętu i procesów powinien współpracować z komputerami nie podpiętymi do firmowej sieci LAN/WAN ani do serwera aplikacji.
- Administrator powinien mieć możliwość tworzenia zestawów komputerowych składających się ze sprzętu, oprogramowania oraz dokumentów niezbędnych do opisania zestawu np. gwarancji, faktur, umów itp. i przyjmowania ich ma majątek IT.
- Wszystkie raporty powinny być dostępne poprzez interfejs HTML.
- Przyjmowany zestaw, oprogramowanie, sprzęt lub licencja powinien być opisany następującymi polami (nazwa, data i godzina przyjęcia, nr faktury, osoba odpowiedzialna za Operację przyjęcia, osoba odpowiedzialna za opiekę, użytkowanie i serwis, stan techniczny tzn. nowy, używany, Magazyn IT, usługa związaną z zakupem składnika, nr ewidencyjny). Dodatkowo zestaw, oprogramowanie, sprzęt lub licencja powinien mieć możliwość przypisania dokumentów, gwarancji, faktur oraz grup do których ten składnik będzie należał.
- Program powinien mieć możliwość przyjęcia określonej liczby zestawów, oprogramowania lub sprzętu o jednakowej konfiguracji.
- Administrator powinien mieć możliwość przesunięcia danego zestawu, oprogramowania, sprzętu lub licencji pomiędzy dowolnymi komputerami, użytkownikami, magazynami, lokalizacjami.
- Administrator powinien mieć możliwość rozdysponowania odpowiedniej ilości danego zestawu, oprogramowania, sprzętu oraz licencji pomiędzy dowolnymi komputerami, użytkownikami, magazynami, lokalizacjami.
- Przyjmowany zestaw komputerowy powinien być rozpoznany przez system i automatycznie opisany stosownymi numerami seryjnymi.
- System w momencie przyjęcia, przesunięcia oraz rozdysponowania składników oraz związanych z tym usług powinien generować protokół. Protokół powinien być opisany polami

(nazwa, informacje kto sporządził, podpisał i zatwierdził, miejsce podpisania, data i godzina, koszt, dodatkowy koszt, nr faktury). Dodatkowo dany protokół powinien mieć możliwość określenia własnych dowolnych pól, wyglądu w formacie rtf oraz dodatkowych załączników.

- Administrator powinien mieć możliwość tworzenia grup elementów np. huby, nośniki cd, centralki telefoniczne, które będą służyły jako szablony do wprowadzania na majątek IT.
- Użytkownicy powinni mieć możliwość importowania z active directory oraz zintegrowany z użytkownikami modułu Rejestracji czasu pracy.
- System powinien posiadać bazę kontrahentów, u których dokonywane są zakupy sprzętu i oprogramowania.
- Raporty min.:
    - globalny przegląd zainstalowanych programów, sprzętu i licencji;
    - zestawienia licencji Freeware oraz innych;
    - porównanie ilości zainstalowanych licencji z wolnymi;
    - lista komputerów z dowolnie zainstalowanym programem, sprzętem oraz wykaz ilościowy;
    - lista komputerów z zainstalowanym systemem operacyjnym oraz wykaz ilościowy ile systemów operacyjnych i w jakiej wersji jest zainstalowanych;
    - lista zabronionych programów, które użytkownik uruchamiał w określonym przedziale czasowym.
- Oprogramowanie powinno automatycznie informować o zmianach w konfiguracji sprzętowo programowej na email.
- Oprogramowanie musi pozwalać nanieść odpowiednie numery seryjne oraz opisy dla urządzeń peryferyjnych w przypadku gdy nie jest możliwe ich automatyczne odczytanie.
- Oprogramowanie musi opisywać licencje polami (nazwa licencji, nr ewidencyjny, licencjodawca, klucz licencyjny, nr licencyjny, rodzaj licencji np. box, molp, cal itp., typ licencji np. dostępowa, grupowa, serwerowa, język licencji, liczba zakupionych licencji, nośnik licencji np. CD-ROM, termin licencji od kiedy do kiedy, termin wsparcia technicznego).
- Licencje oem powinny pozwalać na przypisanie komponentów sprzętowych.
- Każda licencja powinna być opisana umową licencyjną.
- Dowolny program powinien mieć możliwość przypisania kilku licencji np. w przypadku gdy poprzednia licencja wygasła.
- System powinien rozdysponowywać automatycznie tylko tyle licencji ile jest zakupionych, wskazując komputery gdzie nie rozdysponowano licencji ze względu na niedostateczną liczbę.
- System powinien umożliwiać administratorowi wskazanie programów oraz komputerów, które będą podlegały licencji.

- Administrator powinien mieć możliwość przypisania jednej licencji wielu kopii oprogramowania.
- System musi pozwalać na powiadamianie administratora o nieuprawnionych zmianach w konfiguracji sprzętowej np. podmiana pamięci RAM.
- Oprogramowanie lub sprzęt musi mieć możliwość przypisania kodu kreskowego. Kod kreskowy powinien być zgodny ze standardami (code39, code93, codecodabar, codeean128, code128, code2_5_matrix, codeean13, codeean8, codemsi, codepostnet).
- Kod kreskowy powinien mieć możliwość zaprojektowania w przeznaczonym do tego systemie raportowania.
- System powinien posiadać wbudowany moduł pozwalający na tworzenie faktur min polskich oraz unijnych.
- Zestawy komputerowe powinny mieć możliwość wygenerowania karty stanowiska, która powinna posiadać kod kreskowy dla zawierających zestaw podzespołów sprzętowych.
- Karta stanowiskowa powinna mieć możliwość dowolnego zaprojektowania w dedykowanym do tego systemie raportowania który powinien być bezpłatny i zintegrowany z systemem inwentaryzacji.
- Administrator powinien mieć możliwość prowadzenia listy usług, które mogą być kojarzone ze składnikami majątku IT.
- System powinien przypominać administratorowi o zadaniach zaplanowanych.
- System zaplanowanych zadań powinien być opisany polami (nazwa zadania, ważność, osoba wykonująca, osoba nadzorująca, stopień realizacji, typ np. instalacja, konserwacja, data i godzina przypomnienia, data i godzina zakończenia zadania, nazwa usługi związanej z przypomnieniem itp.).
- Raporty powinny wskazywać, które zadania nie zostały wykonane w określonym czasie.
- Wbudowany podstawowy helpdesk z możliwością zgłaszania zadania.
- Licencje powinny mieć możliwość dystrybucji pomiędzy oddziałami firmy, magazynami oraz osobami odpowiedzialnymi za administrowanie.
- Składniki przyjęte na majątek IT powinny mieć możliwość porównania wykazania różnić ilościowych w stosunki do składników automatycznie rozpoznanych przez system.
- Administrator powinien mieć szybką informację o wygasłych lub niezakupionych licencjach dla oprogramowania.
- System powinien ewidencjonować koszty (zakupu urządzeń, kosztów serwisu, kosztu zakupu i modernizacji sprzętu i oprogramowania, kosztów zakupu licencji itp.).
- System powinien tworzyć dowolną ilość magazynów IT oraz dokumentów związanych z operacjami na magazynie IT i przeprowadzać ewidencję ilościowo wartościową.

16. System tworzenia raportów

- Stworzone raporty muszą być bezpłatnie dołączone do aplikacji.
- System raportowania musi być całkowicie bezpłatny zintegrowany z systemem zarządzania i mieć pełne możliwości komercyjnych rozwiązań specjalizowanych w raportowaniu.
- Edytor raportów nie może wymagać zewnętrznych komponentów np. .Net framework, java, IIS, serwera WEB.
- System raportujący powinien mieć profesjonalny edytor projektowy.
- Raporty powinny być eksportowane do różnych formatów (pdf, html, xml, xls, doc, bmp, jpeg, tiff, gif,csv, email oraz na drukarkę).
- Raporty można podłączać do dowolnych baz danych opartych na odbc, OLE DB, ADO np. MS SQLSERWER, ORACLE, DB2 itp.
- Projektant raportów powinien widzieć strukturę bazy danych np. dostępne tabele.
- Tworzone raporty można wyposażyć w wykresy 2d i 3d.
- System powinien mieć wbudowane środowisko do tworzenia raportów w oparciu o język SQL, C++ script, basicscript, jscript, pascalscript itp. wraz z odpowiednimi narzędziami uruchamiania i debugowania.
- Do raportu można nanieść komponenty (takie jak tekst, obrazek, linia, wyrażenie matematyczne, wstęgę, pod raport, wykres, kontrolkę richedit i ole, kod kreskowy itp., html, tabele, stopki, nagłówki, wstęgi podrzędne).
- Dowolne umieszczone w raporcie komponenty można przemieszczać, wyrównywać do krawędzi innych kontrolek i okna, podpinać do źródeł danych, zawijać, tworzyć kotwice, dopasowywać szerokość kolumn i wierszy w tabelach, kolorować, pogrubiać tekst itp.
- Na raportach można umieszczać zmienne, wyrażenia i funkcje matematyczne, tekstowe, agregujące, klasy.
- System raportowania powinien umożliwiać tworzenie raportów typu (główny-szczegółowy, lista, tabela krzyżowa, outline, zagnieżdżony, grupowany typu drill, wielostronicowy, zawierający formularze i okna dialogowe).Dodatkowo do każdego rodzaju raportu system powinien obsługiwać zdarzenia np. zdarzenie ładowania raportu.
- Zawarte w raporcie kolumny i tabele w sposób wizualny powinny być modelowane np. tworzenie relacji itp. oraz generować odpowiedni skrypt SQL.

Raporty powinny mieć możliwość zapisywania, otwierania, dziedziczenia względem innych raportów oraz szablonów.