Załącznik nr 4

Numer referencyjny: SO.2710.2.2024

Zamawiający posiada licencje na oprogramowanie e-auditor firmy BTC od 2012 r. Licencja obejmuje 150 stanowisk i 2 Administratorów. W niniejszym postepowaniu Zamawiający oczekuje przedłużenia wsparcia technicznego dla posiadanej licencji oraz rozbudowy funkcjonalności posiadanego oprogramowania lub dostarczenia całościowo alternatywnego oprogramowania o parametrach wyszczególnionych w niniejszym dokumencie.

1. Przedłużenie subskrypcji na posiadane oprogramowanie E-auditor wraz z prawem aktualizacji do najnowszej wersji systemu do 30.06.2026
2. Rozszerzenie funkcjonalności oprogramowania e-audytor firmy BTC o funkcje systemu zgłoszeń helpdesk dla 2 Administratorów
3. Rozszerzenie funkcjonalności oprogramowania oprogramowania e-audytor BTC o oprogramowanie przeciwdziałające wyciekowi danych (DLP)
4. Wszystkie elementy systemów muszą ze sobą współpracować w zakresie wymiany danych.
5. Wykonawca dokona instalacji, konfiguracji i wdrożenia dostarczonych systemów wraz z przeszkoleniem Administratorów Zamawiającego

# SYSTEM DO ZARZĄDZANIA INFRASTRUKTURĄ IT

## Architektura / budowa

* 1. System musi umożliwić bezproblemową i stabilną obsługę 150 Klientów jednocześnie.
  2. Architektura / budowa:
     1. Klient – 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).
     3. Panel pracownika – aplikacja webowa, niewymagająca dodatkowego logowania, dostępna dla pracowników, udostępniająca wybrane dane z konsoli administracyjnej oraz pozwalająca na interakcję z pracownikiem w wybranych obszarach.
     4. Serwer – oprogramowanie odpowiadające za utrzymywanie komunikacji i wymianę danych z Klientami.
     5. Baza danych pracująca na silniku Microsoft SQL Server w wersjach wyspecyfikowanych poniżej.
  3. Konfiguracja Architektury:
     1. Komponenty systemu (Klient, konsola administracyjna, serwer, baza danych) aktualizują się automatycznie poprzez bezpieczne połączenie.
     2. System zawiera mechanizmy automatycznej konserwacji zgodnie z harmonogramem.

## 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. Edge FireFox, Chrome, Opera).
  2. Klient musi działać na systemach 32 i 64 bitowych: Windows Server 2012/2012R2/2016/2019/2022, Windows 7/8/8.1/10/11, 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.
     1. Klient wspiera poniższe przeglądarki internetowe w zakresie monitorowania aktywności użytkownika w sieci: Opera wersja 63.0.3368.94, Chrome wersja 77.0.3865.90, FireFox wersja 69.0.2
  3. Serwer musi działać na systemach 64 bitowych: Windows Server 2016/2019/2022, Windows 7/8/8.1/10/11.
  4. Serwer www musi być oparty o platformę Microsoft 64 bit (Windows Server 2016/2019/2022, Windows 10 oraz Java 8 (JRE lub JDK), Apache Tomcat 9.
  5. Baza danych musi działać na silniku Microsoft SQL Server 2014/2016/2017/2019/2022 w wersji 64 bitowych zarówno komercyjnych jak i bezpłatnych (np. Microsoft SQL Server Express Edition).
  6. System musi mieć możliwość pracy w środowisku wirtualnym Microsoft Hyper-V oraz VMWare.

## 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. System musi umożliwiać import danych z CSV, Excel, Microsoft SQL Server, MySQL, PostgreSQL
  3. System zapewnia integrację z modelem LLM.

## Funkcjonalności systemu zarządzania infrastrukturą IT

* 1. Funkcjonalność Klienta
     1. System musi umożliwiać pełne zdalne zarządzanie Klientami, obejmujące uruchamianie i wyłączanie, zmianę konfiguracji Klienta, inicjowanie skanowania oraz wykonanie poleceń systemowych. Klient powinien wyświetlać komunikaty w HTML z dokładnymi danymi o czasie wyświetlenia i użytkowniku.
  2. Funkcjonalność konsoli administracyjnej.
     1. Konsola administracyjna musi być wielojęzyczna (polski i angielski) i oferować intuicyjny interfejs z pełnym zestawem funkcji zarządzania (dodawanie, modyfikowanie, usuwanie). Musi także zawierać co najmniej 140 różnorodnych dashboardów, w tym dashboardy użytkownika, prezentujące parametry infrastruktury, sieci oraz bezpieczeństwa. Użytkownicy powinni mieć możliwość samodzielnego konfigurowania dashboardów użytkownika, a dashboardy sieciowe i bezpieczeństwa muszą zawierać szczegółowe widżety z informacjami o stanie usług i bezpieczeństwie.
     2. W konsoli powinna istnieć funkcja filtrowania danych na dashboardach oraz możliwość personalizacji interfejsu przez użytkownika, w tym definiowanie własnych pól, filtrów i widoków, z zachowaniem tych ustawień pomiędzy sesjami. Konsola musi także umożliwiać definiowanie poziomów uprawnień dla użytkowników i grup, z opcją dziedziczenia oraz integrację z Active Directory dla zarządzania dostępem.
     3. Konsola powinna posiadać zaawansowane funkcje zarządzania rekordami, w tym wykonanie poleceń na wielu rekordach jednocześnie oraz dostęp do szczegółowych informacji o pracy urządzeń.
  3. Funkcjonalność panelu pracownika
     1. Panel pracownika systemu musi automatycznie uruchamiać się i autoryzować przy logowaniu użytkownika, z możliwością definiowania zakresu dostępnych informacji przez administratora dla poszczególnych grup pracowników. Panel kierownika powinien dodatkowo agregować i analizować dane z paneli pracowników. Informacje w panelu muszą być organizowane w logiczne sekcje, które można indywidualnie lub grupowo włączać i wyłączać przez administratora.
  4. Zarządzanie licencjami
     1. System musi umożliwiać kompleksowe zarządzanie licencjami w różnych modelach i strukturach organizacyjnych, w tym audyty, zarządzanie oprogramowaniem i oprogramowaniem zabronionym, oraz przypisywanie i rozliczanie różnych typów licencji. Musi także rejestrować historię licencji oraz zapewniać funkcje inwentaryzacji i zdalnej dezinstalacji oprogramowania.
  5. Wzorce aplikacji i pakietów
     1. System powinien posiadać rozbudowaną bazę wzorców oprogramowania, umożliwiać definiowanie własnych wzorców i automatycznie importować nowe wzorce od producenta. Musi także dostarczać szczegółowe informacje o zainstalowanych pakietach i ich wykorzystaniu, w tym edycje Microsoft Office.
  6. Inwentaryzacja sprzętu komputerowego i urządzeń.
     1. System musi oferować rozbudowane funkcje inwentaryzacji sprzętu komputerowego, włączając automatyczną inwentaryzację zarówno w sieci lokalnej jak i zdalnej, szczegółowe skanowanie komponentów (np. RAM, monitory, dyski twarde) oraz zarządzanie informacjami o zainstalowanym sprzęcie. Powinien także umożliwiać ewidencję zmian konfiguracji sprzętu, identyfikować i klasyfikować urządzenia podłączane do komputerów oraz monitorować historię ich podłączeń.
  7. Inwentaryzacja urządzeń sieciowych.
     1. System musi posiadać zdolności do identyfikacji urządzeń sieciowych. Wymagane jest posiadanie skanera sieci i SNMP, które automatycznie zbierają dane, analizują jakość połączeń i identyfikują urządzenia na sieci. System powinien także umożliwiać zdalną instalację Klientów i generowanie map sieci.
  8. Inwentaryzacja sprzętu.
     1. System musi umożliwiać wszechstronną inwentaryzację sprzętu, włączając urządzenia inne niż komputery (np. drukarki, routery). Musi zapewniać zarządzanie dokumentacją związaną z urządzeniami, monitorować ich ruch oraz przypominać o terminach gwarancji i umowach utrzymaniowych.
  9. Ochrona danych (DLP)
     1. Ochrona danych (DLP) musi obejmować automatyczne tworzenie listy podłączanych do komputerów urządzeń USB i ich klasyfikację. System powinien dostarczać informacje o historii użytkowania urządzeń zewnętrznych oraz umożliwiać zarządzanie dozwolonymi do użytku urządzeniami USB zgodnie z zdefiniowanymi regułami.
  10. Szyfrowanie dysków wewnętrznych oraz zewnętrznych
      1. System musi obsługiwać kompleksowe szyfrowanie dysków wewnętrznych i zewnętrznych USB, z wykorzystaniem BitLocker i różnych metod szyfrowania, takich jak XTS\_AES\_256 i AES\_128. Musi umożliwiać zdalne zarządzanie procesem szyfrowania/deszyfrowania, w tym masowe operacje na partycjach systemowych i niesystemowych, zarówno lokalnie, jak i zdalnie (poza NATem). Klucze szyfrujące są przechowywane i chronione w konsoli administracyjnej, dostępne tylko po uwierzytelnieniu administratora. Proces szyfrowania odbywa się w sposób niewidoczny dla użytkownika i nie może być przez niego przerwany, z wyjątkiem stanów hibernacji i wyłączenia systemu, po których jest automatycznie kontynuowany.
  11. Zdalna administracja komputerami
      1. System musi oferować kompleksową zdalną administrację komputerami, włączając w to automatyczne wykonywanie dowolnych poleceń (np. zarządzanie aplikacjami, plikami, rejestrami systemowymi) oraz zarządzanie cyklicznymi zadaniami z harmonogramem. Powinien obsługiwać technologię Intel vPro dla zdalnej konfiguracji i zarządzania, a także pozwalać na zdalne przejęcie kontroli nad komputerem za pomocą technologii Ultra VNC, umożliwiając operowanie na wielu sesjach jednocześnie. System powinien integrować zaawansowane mechanizmy skryptowe wspierane przez AI dla automatycznego generowania poleceń oraz umożliwiać zarządzanie i tworzenie zadań cyklicznych z różnorodnymi opcjami cykliczności i zakończenia.
  12. System musi umożliwiać zdalne w technologii WEBRTC.
      1. System musi zapewniać zdalne zarządzanie komputerami przy użyciu technologii WEBRTC, umożliwiając jednoczesne połączenia z wieloma urządzeniami. Powinien oferować funkcje takie jak przejęcie kontroli nad pulpitami, zarządzanie plikami, uruchamianie i zarządzanie aplikacjami oraz instalowanie oprogramowania i aktualizacji. System powinien umożliwiać konfigurację połączeń WEBRTC, w tym instalację i konfigurację odpowiednich serwerów i portów. Dodatkowo, system powinien obsługiwać różne tryby przejęcia sesji, włączając opcje z lub bez zgody użytkownika, a także umożliwiać nagrywanie i zarządzanie sesjami połączeń, w tym wykonywanie zrzutów ekranu i nagrywanie sesji. System powinien również wspierać różnorodne konfiguracje wyświetlania i jakości sesji, a także umożliwiać uruchomienie do 12 sesji na jednym ekranie.
  13. System musi zezwalać na wykonywanie zapytań WMI bez zdalnego połączenia do urządzenia.
  14. System musi zezwalać na edycję rejestrów urządzenia bez wykorzystania zdalnego połączenia pulpitu.
  15. Zdalne Zarządzanie Zaporą (Firewall)
      1. System musi umożliwiać zdalne zarządzanie zaporą sieciową (firewall) globalnie w infrastrukturze, co obejmuje monitorowanie jej stanu w czasie rzeczywistym, definiowanie złożonych zasad zapory z centralnego panelu administracyjnego oraz szybkie identyfikowanie i reagowanie na potencjalne zagrożenia sieciowe.
  16. Automatyzacja
      1. System musi oferować możliwość ustalania harmonogramu dla czynności konserwacyjnych, naprawczych i porządkujących, z opcją ustalania częstotliwości i parametrów wejściowych dla każdej czynności oraz możliwością ich zatrzymania lub uruchomienia. Dodatkowo, system musi posiadać mechanizmy automatyzacji takie jak wykonywanie kopii bezpieczeństwa, identyfikacja aplikacji i pakietów, porządkowanie bazy danych oraz usuwanie nadmiarowych danych. System również powinien wysyłać alerty o zdarzeniach takich jak nowe komputery w bazie danych, braki w licencjach i inne zdarzenia krytyczne dla infrastruktury IT.
  17. Zarządzanie magazynem IT
      1. System musi umożliwiać efektywne zarządzanie magazynem IT, włączając obsługę dowolnej ilości magazynów w różnych lokalizacjach oraz obsługę dokumentów magazynowych typu PZ, RW, WZ, i inne. System powinien prowadzić ewidencję materiałów w magazynach zgodnie z metodą FIFO. Ponadto, system powinien umożliwiać automatyczne łączenie dokumentów magazynowych z zasobami systemu oraz zapewniać przegląd wszystkich dokumentów.
  18. Repozytorium
      1. Konsola administracyjna systemu musi być wyposażona w repozytorium dokumentów dowolnego typu, które umożliwia dodawanie nowych dokumentów, przeszukiwanie. Repozytorium powinno także umożliwiać definiowanie kontenerów na dokumenty, co ułatwia organizację i zarządzanie dokumentacją.
  19. Kody kreskowe
      1. System musi wspierać obsługę kodów kreskowych jedno i dwuwymiarowych, umożliwiając parametryzację kodu pod względem wielkości i atrybutów graficznych. System powinien umożliwiać podgląd oraz wydruk kodów kreskowych.
  20. System musi posiadać możliwość eksportu / importu treści.
  21. System szkolenia pracowników za pomocą filmów wideo.
      1. System musi oferować szkolenia pracowników za pomocą filmów wideo, z dostępem do biblioteki filmów, która może być rozbudowywana przez administratora. Biblioteka powinna umożliwiać obsługę filmów o minimalnych parametrach 1280 x 720px i 30 klatek na sekundę w formacie mp4. System powinien pozwalać na zdefiniowanie listy filmów dla wybranej grupy pracowników, z możliwością ustawienia szkoleń jako cykliczne. Każdy pracownik powinien mieć dostęp do swojej listy filmów szkoleniowych w panelu pracownika, z informacjami o stopniu ich przeglądnięcia. Filmy powinny być zabezpieczone przed przewijaniem, aby zapewnić pełne ich oglądanie, a po zakończeniu szkolenia system automatycznie generuje certyfikat, który może być modyfikowany, pobierany indywidualnie lub masowo, lub wysyłany emailem.
  22. Monitorowanie drukarek sieciowych i wydruków
      1. System musi umożliwić monitorowanie i zarządzanie wydrukami z dowolnej drukarki (lokalnej czy sieciowej), rejestrując szczegółowe informacje o każdym wydruku, w tym koszty, dzięki wbudowanemu cennikowi. System powinien również prognozować przyszłe koszty drukowania oraz pozwalać na zarządzanie drukarkami według różnych parametrów, w tym statusu i materiałów eksploatacyjnych.
  23. Monitorowanie stron www
      1. System musi oferować monitorowanie aktywności internetowej użytkowników na różnych przeglądarkach, nawet przy szyfrowanych połączeniach (https), rejestrując detale takie jak adresy IP, czas połączenia, a także analizując treści stron za pomocą algorytmów sztucznej inteligencji do klasyfikacji i kontroli treści.
  24. Monitorowanie serwerów WWW
      1. System musi zapewniać monitorowanie wybranych serwerów WWW, prezentując informacje o ich statusie i aktywności, umożliwiając analizę treści stron oraz graficzną prezentację danych związanych z ich działaniem, w tym czasem odpowiedzi i aktywnością w określonym okresie.
  25. Monitorowanie dziennika zdarzeń
      1. System musi posiadać zdolność do monitorowania dziennika zdarzeń komputerów, umożliwiając definiowanie i filtrowanie zdarzeń według różnych kategorii.
  26. System musi umożliwiać monitorowanie komunikatów Syslog.
  27. Monitorowanie pracy komputerów
      1. System musi oferować monitorowanie pracy komputerów, w tym dat startu i zakończenia pracy, logowania użytkowników, a także zdalne monitorowanie sesji połączeń, rejestrując szczegóły takie jak adresy IP i dane użytkowników.
  28. Monitorowanie uprawnień ACL
      1. System musi umożliwić skanowanie i monitorowanie uprawnień ACL, oferując szczegółowe raporty, automatyczną aktualizacją danych i filtrami do zarządzania informacjami.
  29. Monitorowanie sensorów
      1. System musi integrować monitoring warunków środowiskowych za pomocą sensorów po SNMP, umożliwiając graficzną prezentację danych, wysyłanie alertów.
  30. Repozytorium CMDB
      1. System musi posiadać zintegrowane repozytorium CMDB, umożliwiające zarządzanie zasobami IT, w tym szczegółowe informacje o użytkownikach, urządzeniach, licencjach, a także o oprogramowaniu i jego licencjach, z możliwością importu i eksportu danych.
  31. Worktime manager
      1. System musi umożliwiać monitorowanie i analizę czasu pracy użytkowników, z możliwością definiowania grup przypisanych do przełożonych i prezentacji szczegółowych danych o aktywności użytkowników w formie widżetów i danych analitycznych. Informacje o czasie pracy, sesjach, aktywności w aplikacjach oraz produktywności powinny być możliwe do udostepnienia w panelu pracownika.
  32. Raportowanie i eksport danych
      1. System musi oferować zaawansowane możliwości raportowania i eksportu danych, umożliwiając wyeksportowanie informacji do różnych formatów, w tym xls, csv, html, oraz graficznych. Powinien także wspierać generowanie wieloparametrycznych raportów z możliwością stosowania filtrów, obsługę wieloinstancyjności raportowania oraz integrację z narzędziami do tworzenia raportów takimi jak SAP Crystal Reports i Stimulsoft, obejmując co najmniej 150 zdefiniowanych raportów. Dodatkowo, system musi posiadać możliwość konfiguracji harmonogramu umożliwiającego cykliczne wysyłanie raportów oraz zapisywanie ich w dowolnym miejscu, z automatycznym generowaniem raportu w formacie PDF jako wynikiem wykonania harmonogramu.
  33. System musi zapewnić interfejs API.
      1. System musi oferować rozbudowany interfejs API, umożliwiający komunikację za pomocą REST API. Musi on zapewniać szyfrowaną komunikację z użyciem protokołu TLS 1.3 oraz możliwość tworzenia złożonych requestów JSON. Klucze zabezpieczeń powinny być modyfikowalne i mogą mieć co najmniej 32 znaki.
  34. Powiadomienia
      1. System musi umożliwiać generowanie różnorodnych powiadomień, w tym alertów w konsoli, e-maili oraz wiadomości SMS, z możliwością edycji treści powiadomień i definiowania grup odbiorców. Powinien obsługiwać automatyczne wywoływanie zadań i integrować się z CMD oraz Windows PowerShell, zapewniając co najmniej 30 predefiniowanych powiadomień oraz możliwość ich personalizacji.
  35. Bezpieczeństwo
      1. System musi zapewniać rozbudowane funkcje bezpieczeństwa, w tym definicję i zarządzanie prawami dostępu oraz zaawansowane opcje uwierzytelniania. Wymaga silnych haseł, obsługuje wieloskładnikowe uwierzytelnianie i posiada mechanizmy szyfrowania danych.

1. Wsparcie i pomoc
   * 1. Pomoc techniczna
        1. Musi być świadczona co najmniej w dni robocze w godzinach od 8.00-16.00.
        2. Utrzymaniem Oprogramowania jest zapewnienie aktualizacji Oprogramowania (asysta techniczna) oraz nieprzerwanego działania Oprogramowania (usługi SLA), jak również zapewnienie świadczenia innych usług wspomagających korzystanie z Oprogramowania.
        3. Czas trwania usługi SLA od dnia zakupu **do 30.06.2026 r.**

**System helpdesk**

**Architektura/Wsparcie**

* SLA
  + Czas trwania usługi SLA wynosi od dnia zakupu do 30.06.2026
* Ilość dostępów administracyjnych
  + System musi posiadać 2 dostępy administracyjne (tzw. użytkownik nazwany).

# Architektura / wymagania systemowe

* 1. Musi być kompletnym systemem wspierającym pracę działu wsparcia technicznego (helpdesk). System musi zawierać moduły: zarządzanie zgłoszeniami, ewidencja magazynowa, zakupy IT, zarządzanie umowami serwisowymi, portal pomocy technicznej oraz baza wiedzy.
  2. System musi być w pełni funkcjonalną aplikacją internetową (webową). Konsola administracyjna musi działać na dowolnej przeglądarce stron WWW zgodnej z HTML5 (np. Edge, Firefox, Chrome, Opera).
  3. Bazę danych systemu musi stanowić postgresql.
  4. System musi współpracować z czytnikiem i drukarką kodów paskowych.
  5. System musi być zgodny z ITIL v4.
  6. System musi zapewniać integrację z Active Directory.
  7. System musi zapewniać integrację z systemem zarządzania zasobami IT.
  8. System musi posiadać co najmniej 1 dostęp administracyjny (tzw. użytkownik nazwany) umożliwiające jednoczesne działania serwisantów w konsoli systemu.
  9. System musi zapewnić interfejs API:
     1. System musi udostępniać możliwości komunikacji z systemem za pomocą REST API.
     2. Komunikacja z REST API musi odbywać się w sposób szyfrowany min. Protokołem TLS 1.3 i chroniony kluczem alfanumerycznym.
     3. System musi zapewniać możliwości modyfikacji i dostosowania klucza zabezpieczeń REST API i pozwalać na ustanowienie klucza o długości co najmniej 32 znaków.
     4. System musi pozwalać na tworzeni requestów obsługujących parametry w formacie JSON.
     5. W ramach REST API konieczne musi być możliwość pobierania danych ze wszystkich tabel systemu, zawierających dane merytoryczne.
     6. System musi przyjmować requesty pozwalające na umieszczanie danych w systemie za pomocą REST API.
     7. System musi dopuszczać komunikację złożoną, za pomocą sekwencji requestwów REST API.
     8. System musi pozwalać na automatyczną komunikację za pomocą REST API z innymi systemami z wykorzystaniem składni API systemu.

# Zakres funkcjonalny systemu:

* 1. Zarządzanie Incydentem.
  2. Zarządzanie Problemem.
  3. Zarządzanie Zmianą.
  4. Baza konfiguracji CMDB.
  5. Zarządzanie umowami SLA.
  6. Portal Pomocy Technicznej.
  7. Baza wiedzy.
  8. Zarządzanie magazynami.
  9. Zarządzanie umowami serwisowymi.
  10. Zarządzanie zakupami.
  11. Ankietowanie użytkowników.
  12. Raportowanie zgłoszeń z filtrami: urządzenie, użytkownik, jednostka organizacyjna, czas naprawy, koszt użytych do naprawy elementów, zgłoszenia w określonym przedziale czasowym.
  13. Webowa platforma zgłoszeń sygnalistów.

# Moduł Zarządzanie Incydentem musi obsługiwać:

* 1. Różne typy zgłoszeń.
  2. Dokładną rejestrację i klasyfikację incydentów.
  3. Diagnostykę i rozwiązywanie zgłoszeń z wykorzystaniem modułu zarządzania wiedzą.
  4. Szczegółowe raporty trendów w incydentach.
  5. Ewidencję czasu pracy serwisanta.
  6. Zatwierdzanie rozwiązania incydentu przez użytkownika.
  7. Pełną historię zgłoszenia.
  8. Możliwość ustawienia automatycznej odpowiedzi na zgłoszenia użytkowników za pomocą sztucznej inteligencji.

# Moduł Zarządzanie Problemem musi obsługiwać:

* 1. Rejestracja nowego problemu lub powiązanie wielu incydentów w jeden problem.
  2. Diagnostyka powiązanych problemów i poszukiwanie głównej przyczyny incydentów.
  3. Tworzenie rozwiązań tymczasowych i docelowych.
  4. Szczegółowe raporty trendów – działania prewencyjne.
  5. Analizy, rozwiązania i zadania dodatkowe.

# Moduł Zarządzanie Umowami SLA w zakresie oprogramowania musi obsługiwać:

* 1. Definiowanie reguł SLA ze względu na użytkownika, jednostkę organizacyjną przedsiębiorstwa, kategorię czy priorytet.
  2. Automatyczną aktualizację zgłoszeń aby zapewnić zgodny z SLA czas rozwiązania.
  3. Czuwanie nad zakończeniem rozwiązania problemu w zdefiniowanym uprzednio przedziale czasu i w razie potrzeby zastosowanie mechanizmu eskalacji (do 4 poziomów).
  4. Pomiar jakości SLA – raportowanie.
  5. Powiadomienia serwisantów o zbliżającym się końcu czasu przeznaczonego na rozwiązanie zgłoszenia.

# Moduł Portal Pomocy Technicznej musi obsługiwać:

* 1. Przyjazny interfejs i łatwość tworzenia zgłoszeń.
  2. Szablony standardowych zgłoszeń.
  3. Możliwość sprawdzania statusu zgłoszeń w realizacji.
  4. Wbudowana baza wiedzy.
  5. Dostęp do zgłoszeń historycznych.

# Moduł Baza wiedzy musi obsługiwać:

* 1. Dostęp do tworzonej przez dział IT bazy 24h/7d.
  2. Indeksowanie przy użyciu słów – kluczy.
  3. Rozdzielenie bazy wiedzy pomiędzy serwisantów (IT) i użytkowników końcowych z dostępem tylko do prostych rozwiązań (z którymi mogą sobie sami poradzić).
  4. Grupowanie rozwiązań wg tematów.
  5. Dostęp do "najbardziej popularnych" i "ostatnio dodanych" rozwiązań.

# Moduł Raportowanie musi obsługiwać:

* 1. Obsługa raportów w standardzie Stimulsoft lub zgodnym.
  2. Raporty parametryczne z parametrami statycznymi i dynamicznymi.
  3. Predefiniowane raporty obejmujące całokształt funkcjonalności zgodne z ITIL v. 4.

# Zarządzanie zmianą musi obsługiwać :

* 1. Planowanie zmiany i harmonogramu projektów w webowym interfejsie GUI.
  2. Możliwości ustawiania schematów zatwierdzeń zmiany.
  3. Możliwości przypisania wielu osób do schematu zatwierdzeń zmiany.
  4. Obsługa wielu zmian i projektów w oparciu o wspólny schemat kalendarza, umożliwiający kontrolę przebiegu zmiany.
  5. Możliwości modyfikacji z poziomu GUI elementów projektu i formularza zmiany.
  6. Automatyczne powiadomienia oraz system zatwierdzeń, wysyłane do właściwych osób.
  7. Możliwość ograniczenia widoku zmian i planowania ze względu na uprawnienia osób.
  8. Możliwości powiązania zmian z systemem ticketowym oraz zasobami systemu ticketowego.
  9. Możliwości śledzenia przebiegu zmiany przez supervisora.
  10. Możliwość zatwierdzenia przez osobę bez dostępu do systemu, o ile została uwzględniona w schemacie zatwierdzeń.

# Platforma zgłoszeń sygnalistów musi obsługiwać:

* 1. Webową i powszechnie dostępną, nie wymagającą logowania platformę dostępu dla sygnalistów.
  2. Platformę publikacji dokumentów firmowych.
  3. Szyfrowaną dwukierunkową komunikację pomiędzy sygnalistą a osobą obsługującą na każdym etapie zgłoszenia, bez pobierania jakichkolwiek danych od sygnalisty, w tym bez pobierania adresu mailowego.
  4. Możliwość załączania plików do formularza zgłoszenia.
  5. Modyfikowalny formularz zgłoszenia, dostosowywany z poziomu GUI systemu przez administratora nieposiadającego fachowej wiedzy informatycznej.
  6. Możliwość ustawienia interaktywnych formularzy zgłoszeń dla poszczególnych kategorii zgłoszeń.
  7. Możliwość ustawienia minimalnych wymagań formularza zgłoszenia.
  8. Zabezpieczenia captcha dla komunikacji z sygnalistą.
  9. Możliwość dodania klauzuli RODO.
  10. Interaktywny widok zgłoszeń sygnalistów.
  11. Oddzielny od systemu ticketowego system uprawnień i obsługi administracyjnej.
  12. Zabezpieczone powiadomienia o próbach ingerencji w uprawnienia użytkowników systemu.
  13. Możliwość integracji z systemami obsługi wniosków.

# Bezpieczeństwo

* 1. System wyposażony jest w mechanizmy definicji praw dostępu do poszczególnych widoków danych i opcji w konsoli administracyjnej.
  2. System umożliwia zablokowanie komunikacji z serwerem producenta w celu wyłączenia aktualizacji.
  3. System umożliwia dostarczenie aktualizacji w formie offline.
  4. Uwierzytelnianie do systemu jest 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 kont LDAP,
     6. Za pośrednictwem kont CAS,
  5. System umożliwia definiowanie poziomu uprawnień dla grupy oraz użytkownika (odczyt, zapis, kasowanie) do wszystkich widoków danych oraz wybranych elementów struktury organizacyjnej, wyposażony jest w opcję dziedziczenia uprawnień. Odebranie praw do widoku lub zakładki na widoku powoduje ukrycie opcji.
  6. Lista użytkowników / administratorów systemu jest 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.
  7. System posiada mechanizmy automatycznego wykonywania kopii bezpieczeństwa w zadanych interwałach czasowych w formie kopii przyrostowej i nie przyrostowej oraz może udostępniać informacje o rezultacie wykonania kopii.
  8. System pobiera dane z widoków (ang. View) zdefiniowanych w bazie danych a nie bezpośrednio z tabel bazy danych.
  9. 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).
  10. System zapewnia mechanizmy zapewniające integralność, poufność i dostępność przechowywanych informacji.

# Pomoc techniczna

* 1. Pomoc techniczna
     1. Musi być świadczona co najmniej w dni robocze w godzinach od 8.00-16.00.
     2. Utrzymaniem Oprogramowania jest zapewnienie aktualizacji Oprogramowania (asysta techniczna) oraz nieprzerwanego działania Oprogramowania (usługi SLA), jak również zapewnienie świadczenia innych usług wspomagających korzystanie z Oprogramowania.
  2. Czas trwania usługi SLA wynosi od dnia zakupu **do 30.06.2026 r.**
  3. Usługi Utrzymania Oprogramowania obejmują:
     1. asystę techniczną,
     2. świadczenie usług SLA, w ramach, których realizowana jest:
        1. obsługa zgłoszeń w zakresie:
           1. reakcja na zgłoszenia błędów w określonym czasie reakcji;
           2. dokonywanie analizy przyczyn błędów;
           3. zapewnianie obejścia dla błędów występujących z przyczyn leżących po stronie oprogramowania podmiotów trzecich;
           4. zapewnianie obejścia dla błędów występujących z przyczyn leżących po stronie infrastruktury zamawiającego;
           5. usuwania błędów w czasie naprawy;
           6. usuwania błędów występujących z przyczyn leżących po stronie oprogramowania podmiotów trzecich – po udostępnieniu odpowiedniej aktualizacji przez producenta tego oprogramowania oraz jej uzyskaniu – w czasie naprawy;
           7. zapewnienia dostępności Oprogramowania.

System DLP

System zapobiegania wyciekom danych i informacji (DLP).

1. Architektura / budowa
   1. System musi umożliwić bezproblemową i stabilną obsługę 150 komputerów jednocześnie.
   2. System musi posiadać 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). Konsola musi pozwalać na realizację pełnego zarządzania systemem oraz komputerami, musi być wyposażona w mechanizmy do edycji/modyfikacji i analizy danych oraz zawierać wbudowany mechanizmy raportowania. Nie jest dopuszczalne stosowanie aplikacji webowej do przeglądania danych oraz innej aplikacji do wprowadzania/edycji danych czy też realizacji innych funkcji systemu.
      3. Serwer – oprogramowanie odpowiadające za utrzymywanie komunikacji i wymianę danych z agentami.
      4. Baza danych musi pracować na silniku Microsoft SQL Server.
      5. Wszystkie komponenty systemu muszą się aktualizować samodzielnie za pośrednictwem bezpiecznego połączenia z serwerem 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 wewnętrznej funkcjonalności systemu. 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 aktualizacją.
      6. System musi w sposób w pełni automatyczny z wykorzystaniem serwera aktualizacji producenta aktualizować niezbędne bazy wzorców, polityk, pomoc i inne wbudowane słowniki.
      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 interfejsu konsoli, w postaci sparametryzowanego wewnętrznie pliku msi (ustawione zmienne np. adres IP, port serwera) gotowego do zainstalowania
      9. Agent musi być możliwy do zainstalowania za pośrednictwem MS Active Directory lub manualnie.
      10. Agent musi pracować w trybie niewidocznym dla użytkownika (jako usługa systemowa).
      11. System powinien umożliwiać generowanie unikatowego identyfikatora agenta (powtarzalnego dla danego komputera) na podstawie kombinacji parametrów wybranych przez użytkownika systemu spośród: nazwy producenta BIOS, numeru seryjnego komputera, system UUID, nazwy komputera, definiowalnego ciągu znaków lub losowego ciągu znaków.
      12. Agent musi mieć definiowalny priorytet pracy (ABOVE\_NORMAL, NORMAL, BELOW\_NORMAL, IDLE).
      13. Agent musi wspierać do sześciu różnych adresów serwera rozumianych jako adresy w sieci lokalnej, rozległej (VPN) oraz za NATem i musi potrafić wykorzystać adres dostępny z puli adresowej w dowolnym momencie działania, bez konieczności restartu.
      14. System musi umożliwiać komunikację pomiędzy agentami a serwerem w sieciach lokalnych, rozległych, także gdy komputery znajdują się za NATem.
      15. System musi mieć możliwość współpracy komponentów agent i serwer w taki sposób, aby serwer mógł współpracować ze wszystkimi poprzednimi wersjami agentów.
      16. Systemmusi mieć wbudowane mechanizmy automatycznej konserwacji/utrzymania zgodnie ze zdefiniowanym harmonogramem realizujące co najmniej: usuwanie zbędnych danych z systemu o definiowalnych parametrach retencji (w tym dane z monitoringu uruchamianych aplikacji, uruchamianych procesów, odwiedzonych stron www, wydrukowanych dokumentów), indeksowanie bazy danych, kopie bezpieczeństwa przyrostowe i nieprzyrostowe, zmniejszanie bazy danych (tzw. shrink). 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.
2. 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. Edge, Firefox, Chrome, Opera).
   2. Agent musi działać na systemach 32 i 64 bitowych: Windows Server2012/2012R2/2016/2019/2022, Windows 7/8/8.1/10/11, 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 2016/2019/2022, Windows 7/8/8.1/10/11.
   4. Serwer www musi być oparty o platformę Microsoft 64 bit (Windows Server 2012/2012R2/2016/2019/2022, Windows 10, Windows 11) oraz Java 8 (JRE lub JDK), Apache Tomcat 9.
   5. Baza danych musi działać na silniku Microsoft SQL Server 2012/2014/2016/2017/2019 w wersji 64 bitowych bezpłatnej Microsoft SQL Server Express Edition.
   6. System musi mieć możliwość pracy w środowisku wirtualnym Microsoft Hyper-V oraz VMWare.
3. Interfejs
   1. System musi umożliwiać wielokrotny (harmonogram), na życzenie, import użytkowników, struktury organizacyjnej z usługi MS Active Directory, przy czym import struktury organizacyjnej musi następować we wskazane miejsce struktury organizacyjnej systemu.
   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 dowolnego źródła danych, w tym z plików CSV, XLS, XLSX, MS SQL oraz baz danych MS SQL Server, MySQL, PostgreSQL poprzez definiowanie źródła danych, reguł importu (jakie pola/kolumny) oraz posiadać wbudowany harmonogram raportów.
   5. System musi umożliwiać pobieranie danych z komputerów (wyników skanowania) metodą bezpośredniego połączenia, za pośrednictwem serwera pocztowego (MAIL), za pośrednictwem serwera HTTP/HTTPS.
4. Funkcjonalności systemu
   1. System musi monitorować i zapobiegać wyciekom danych (DLP) poprzez bieżące (w czasie rzeczywistym) monitorowanie działań użytkowników wg ściśle zdefiniowanych polityk bezpieczeństwa oraz reguł ich opisujących.
   2. System musi prowadzić szczegółową bieżącą informację o zarządzanych komputerach.
   3. System musi udostępniać podstawowe dane inwentaryzacyjne komputerów, m.in.: procesor, BIOS, pamięć, dyski twarde, tabela smart dysków, sieć, pliki, czas pracy, zdarzenia.
   4. System musi zapewniać automatyczne uruchamianie ochrony zasobów w czasie rzeczywistym zgodnie ze zdefiniowanymi politykami.
   5. System musi zapewniać ciągłą ochronę danych niezależnie od położenia komputera (w sieci lokalnej, sieci VPN, poza siecią).
   6. System musi na bieżąco monitorować i chronić za pomocą odpowiednio zdefiniowanych polityk i reguł dane w ruchu, dane w spoczynku oraz dane w użyciu.
   7. Przez dane w spoczynku rozumie się dane, które nie są (ale mogą być) w ruchu lub w użyciu, wymagają inwentaryzacji i zabezpieczenia.
   8. Przez dane w użyciu należy rozumieć dane, które są aktywnie przetwarzane przez dowolną aplikację i/lub punkt końcowy (komputer). Przykłady danych w użyciu: edycja dokumentu MS Word, Excel, PowerPoint, edycja pliku tekstowego CSV, TXT, tworzenie pliku, przechwytywanie ekranu (screenshot), kopiowanie / wklejanie danych,

Wydruki.

Przez dane w ruchu należy rozumieć dane, które są przesyłane, np. kopiowanie danych (plików) z dysku sieciowego na nośnik USB, kopiowanie danych (plików) z komputera na komputer, przesyłanie danych e-mailem w treści lub w postaci załącznika, pobieranie danych z serwera FTP, przesyłanie danych za pomocą komunikatora.

* 1. System musi w pełni wspierać następujące polityki ochrony danych:
     1. Zdefiniowanie schematu, w którym można określić, które aplikacje są zabronione, zalecane, dodatkowe bądź nieokreślone. Schemat oprogramowania można przypisać do dowolnej grupy komputerów. Mechanizm musi umożliwić automatyczne odinstalowanie oprogramowania, które wg zdefiniowanego schematu jest zabronione.
     2. Oznaczanie na dowolnym komputerze (znakowanie przez agenta) określonych plików wybranymi, niewidocznymi, dowolnie zdefiniowanymi znacznikami będącymi alternatywnym strumieniem danych w pliku.
     3. Znakowanie określonych plików przechowywanych w zasobach serwerów lub udostępnionych zasobach (np. samodzielna macierz dyskowa) wybranymi, niewidocznymi, dowolnie zdefiniowanymi znacznikami, z wykorzystaniem harmonogramu jako alternatywny strumień danych.
     4. Kontrolowanie wykonywania przez użytkowników operacji zrzutu ekranu.
     5. Generowanie automatycznych zrzutów ekranu komputera w ramach ustalonego interwału czasowego wyrażonego w sekundach.
     6. Umożliwienie powiadamianie o przekroczeniu dozwolonego czasu pracy komputera.
     7. Podjęcie działania w momencie uruchomienia określonego procesu.
     8. Monitorowanie określonych typów urządzeń przenośnych.
     9. Monitorowania i blokowania operacji (otwieranie/ usuwanie/ tworzenie/ zapis/ zmiana nazwy) na plikach.
     10. Zarządzanie dostępem do sieci społecznościowych, serwisów informacyjnych, blogów, bibliotek, forów dyskusyjnych oraz dowolnych stron www.
     11. Wyświetlanie komunikatu na komputerach użytkowników podczas uruchamiania stacji roboczej. Komunikaty muszą być definiowalne z poziomu konsoli administracyjnej z wykorzystaniem edytora (możliwość utworzenia tabeli, dołączenia obrazu, wstawienia linku).
     12. Monitorowanie danych przesyłanych za pomocą poczty e-mail oraz blokowanie przesyłania plików określonych typów w lokalnej wersji poczty outlook.
     13. Monitorowanie danych przesyłanych do chmury oraz blokowanie synchronizacji plików określonych typów z wybraną chmurą.
     14. Blokowanie lub zezwalanie działania określonym typom urządzeń dostępnych w menedżerze urządzeń.
         1. System musi pozwalać na zarzadzanie dostępem do telefonów komórkowych w trybie pamięci masowej, czytników kart pamięci i pendrive USB.
     15. Podjęcie działań monitorowania i blokowania operacji w momencie próby kopiowania tekstu, zdjęcia czy ścieżki plików do schowka.
     16. Blokowanie sieci ze względu na zdefiniowany typ i maskę sieci WIFI. Polityka musi zapewniać blokowanie dostępu do sieci zarówno otwartych jak i zabezpieczonych.
  2. System musi być wyposażony w mechanizm tworzenia reguł ochrony (DLP) w oparciu o zdefiniowane polityki, obiekty docelowe, nazwy użytkowników, datę ważności polityki.
     1. Obiekty docelowe reguł muszą być definiowalne za pomocą parametrów takich jak: nazwa komputera, adres IP, unikatowy identyfikator agenta, status podłączenia do systemu (online/offline), zainstalowany system operacyjny, nazwę zalogowanego użytkownika, model komputera, producent komputera, dostawca komputera, budżet, z którego zakupiony został komputer, strukturę organizacyjną
  3. Przy definiowaniu obiektów docelowych dla reguł DLP można korzystać ze znaków wieloznacznych.
  4. System musi posiadać funkcjonalności monitorowania, blokowania, powiadomieniu użytkownika o wystąpieniu naruszenia zdefiniowanej polityki oraz pełnego logowania zdarzeń dotyczących polityki dla celów administracyjnych (powiadomienie administratora systemu).
  5. Monitorowanie i ochrona danych
     1. System musi wspierać definiowanie nieograniczonej liczby znaczników (ang. fingerprint) i umożliwiać użycie ich do znakowania danych (plików).
     2. System musi umożliwiać zdefiniowania bądź wykluczenia maski plików do oznakowania z wykorzystaniem znaków wieloznacznych, w konkretnych lokalizacjach lokalnych bądź sieciowych.
     3. Znacznik nie może naruszać struktury pliku, w szczególności sygnatury podpisu cyfrowego, wielkości pliku i musi być niewidoczny dla użytkownika.
     4. Jeden plik może być oznaczony dowolną ilością znaczników.
     5. Zdejmowanie znaczników może być prowadzone w sposób manualny zdalnie przez administratora lub automatycznie, gdy reguła ustali, że znacznik powinien być zdjęty (np. plik w wyniku prowadzonej przez użytkownika edycji nie posiada już danych osobowych).
     6. System musi automatycznie znakować plików tworzone przez zdefiniowane procesy aplikacji, wybranych użytkowników.
     7. System musi mieć możliwość automatycznego ustawiania / usuwania znaczników na plikach (np. txt, doc, docx, xls, xlsx, ppt, pptx) w oparciu o dowolnie zdefiniowaną zawartości (treści) pliku w postaci tekstu i wyrażenia regularnego.
  6. Zrzuty ekranu
     1. System musi obsługiwać wielu ekranów (wiele monitorów podłączonych do jednego komputera).
     2. System musi obsługiwać pulpity wirtualne (logiczny rozmiar pulpitu jest większy niż fizyczny rozmiar ekranu).
     3. System musi mieć możliwość monitorowania/zablokowania wykonania zrzutu ekranu przez użytkownika za pomocą klawiatury.
     4. System musi umożliwiać czytelny podgląd obrazów (zrzutów ekranowych) w konsoli administracyjnej.
  7. Monitorowanie czasu pracy
     1. System musi mieć możliwość zdefiniowania dowolnej ilości reguł dotyczących czasu pracy komputera.
     2. System musi mieć możliwość zdefiniowania zalecanego czasu pracy dla każdego komputera, przy czym czas pracy w każdym dniu tygodnia może być zdefiniowany inaczej.
     3. System musi mieć możliwość automatycznego dołączenia bieżącego zrzutu ekranu do każdego incydentu związanego z przekroczeniem zalecanego czasu pracy.
  8. Uruchamiane procesy i aplikacje
     1. System musi mieć możliwość zdefiniowania dowolnej ilości reguł dotyczących uruchamiania procesu/aplikacji poprzez wykorzystanie maski zawierającej znaki wieloznaczne („\*” oraz „?” zastępujące odpowiednio dowolny ciąg znaków oraz znak pojedynczy).
     2. System musi mieć możliwość dołączenia bieżącego zrzutu ekranu do informacji o incydencie związanym z próbą uruchomienia monitorowanego procesu/aplikacji.
  9. Monitorowanie urządzeń przenośnych
     1. System musi mieć możliwość utworzenia grup urządzeń przenośnych identyfikatora sprzętowego.
     2. System musi automatycznie inwentaryzować (identyfikator sprzętowy, nazwa) podłączane do komputerów urządzenia przenośne.
     3. System musi automatyczne rozpoznawać status zaszyfrowania urządzenia przenośnego.
     4. System musi mieć możliwość wykluczania grup urządzeń przenośnych z monitorowania (tzw. biała lista).
     5. System musi mieć możliwość definiowania dni tygodnia oraz zakresu godzin, w których ma być aktywne monitorowanie urządzeń przenośnych.
     6. System musi mieć możliwość jednoczesnego odczytania wielu identyfikatorów urządzeń przenośnych za pomocą multiplikatora portów USB poprzez wbudowaną do systemu funkcję lub aplikację.
     7. System musi mieć możliwość dołączenia bieżącego zrzutu ekranu do każdego incydentu związanego z użyciem urządzenia przenośnego.
  10. Operacje w systemie plików
      1. System musi monitorować zdarzenia otwarcia, usunięcia, utworzenia, zapisu, zmiany nazwy pliku w całym systemie plików.
      2. System musi mieć możliwość zdefiniowania lokalizacji podlegających oraz wykluczonych z monitorowania oraz pozwalać na zdefiniowanie maski plików podlegających / wykluczonych z monitorowania z użyciem znaków wieloznacznych.
      3. System musi mieć możliwość definiowania maski procesów, dla których dostęp do systemu plików będzie monitorowany.
      4. System musi mieć możliwość stworzenia tzw. białej listy procesów, których dostęp do systemu plików nie będzie monitorowany.
      5. System musi mieć możliwość monitorowania plików w oparciu o założone na pliki znaczniki.
  11. Dostęp do stron WWW
      1. System musi mieć możliwość zdefiniowania maski stron podlegających monitorowaniu / blokowaniu za pomocą znaków wieloznacznych.
      2. System musi mieć możliwość blokowania stron w oparciu o protokół nieszyfrowany (http) oraz szyfrowany (https).
      3. System musi zapewnić wsparcie dla przeglądarek Opera w wersji nie niższej niż 102, Chrome w wersji nie niższej niż 128 oraz Firefox w wersji nie niższej niż 29.
  12. Kanał poczty elektronicznej e-mail
      1. System musi mieć możliwość zdefiniowania maski plików, które będą podlegały monitorowaniu/blokowaniu w zakresie ich użycia (wysyłania) w programach pocztowych za pomocą znaków wieloznacznych.
      2. System musi wspierać rozwiązań poczty oparte o chmurę.
  13. Ochrona dostępu do rozwiązań opartych o chmurę
      1. System musi mieć możliwość zdefiniowania masek plików, które będą podlegały monitorowaniu / blokowaniu w zakresie ich transmisji z lub do rozwiązania opartego o chmurę.
      2. System musi wspierać co najmniej następujące rozwiązania oparte o chmurę: BitTorrent Sync, Box, Copy, Cubby, Dropbox, Google Drive, Knowhow Cloud, Mediafire, Mega, Microsoft OneDrive, Mozy, Spideroak, Strato HiDrive, Tresorit, Own Cloud.
  14. Zabezpieczenia urządzeń
      1. System musi mieć możliwość blokowania użycia grup urządzeń wg nazwy.
      2. System musi mieć możliwość blokowania użycia grup urządzeń wg typu: stacje dysków CD-ROM/DVD, czujniki, czytniki kart inteligentnych, drukarki, GPS, imaging devices, karty graficzne, karty sieciowe, klawiatury, kontrolery dźwięku, wideo i gier, kontrolery IDE ATA/ATAPI, kontrolery IEEE 1394 Host Bus, kontrolery magazynu, kontrolery uniwersalnej magistrali szeregowej, kopie w tle woluminów magazynu, modemy, mysz i inne urządzenia wskazujące, napędy dyskietek, napędy taśmowe, PCMCIA adaptery, porty (COM i LPT), przenośne urządzenia z systemem Windows (WPD), software devices, stacje dysków, urządzenia akumulatorowe, urządzenia biometryczne, urządzenia Bluetooth, urządzenia interfejsu HID, urządzenia IrDA, urządzenia wielofunkcyjne, urządzenia zgodne ze standardem IEEE 1284.4, urządzenie USB, wieloportowe karty szeregowe, urządzenia Windows CE ActiveSync USB, woluminy magazynu, zmieniarki mediów.
      3. System musi mieć możliwość dołączenia bieżącego zrzutu ekranu do informacji o incydencie związanym z zablokowaniem / odblokowaniem urządzenia.
  15. Szyfrowanie urządzeń USB
      1. System musi identyfikować partycje urządzeń USB zaszyfrowane Bitlockerem.
      2. System musi posiadać wbudowane mechanizmy do masowego zdalnego szyfrowania BitLockerem i wspierać metody XTS AES256, XTS AES128, AES256, AES128.
      3. Ochrona danych na urządzeniach USB musi być realizowana przez silne szyfrowanie całej zawartości urządzenia.
      4. System musi umożliwiać zdalne szyfrowanie / deszyfrowanie urządzeń USB oraz prezentować bieżący postęp tego procesu.
      5. Proces szyfrowania odbywa się w sposób przezroczysty dla użytkownika komputera i może być realizowany w czasie jego pracy na komputerze. Szyfrowanie może być wyłączone przez użytkownika.
  16. System musi umożliwiać szyfrowanie / deszyfrowanie urządzeń USB w sieci lokalnej oraz poza NATem
  17. System musi umożliwiać zarządzanie dostępem do urządzeń usb poprzez definiowanie reguł blokujących dostęp do niezaszyfrowanych urządzeń.
  18. Powiadomienia użytkowników
      1. System musi mieć możliwość definiowania treści powiadomienia użytkownika komputera o naruszeniu przez niego polityki lub incydencie, zarówno z aktywnym blokowaniem incydentu (blokada i powiadomienie) jak i bez blokowania (tylko powiadomienie).
      2. System musi mieć możliwość wykorzystania w komunikatach zmiennych systemowych (np. %UserName%, %FileName%, itp.), które w komunikacie dla użytkownika zostają automatyczne zastąpione rzeczywistymi danymi.
  19. Powiadomienia administratorów
      1. System musi prezentować wszystkie incydenty w konsoli administracyjnej oraz powiadamiać administratora o wystąpieniu incydentu za pomocą poczty e-mail w chwili jego wystąpienia.
      2. Treść powiadomienia musi być definiowalna odrębnie dla każdej polityki DLP i musi umożliwiać wykorzystanie zmiennych systemowych (np. %UserName%, %FileName%, itp.), które w wysyłanym komunikacie zostają automatyczne zastąpione rzeczywistymi danymi.
      3. System musi obsługiwać szyfrowane protokoły poczty e-mail.
      4. System musi umożliwiać zdefiniowania dowolnej liczby odbiorców powiadomień.
  20. Zarządzanie politykami bezpieczeństwa
      1. System musi mieć możliwość konfiguracji i instalacji dowolnej ilości reguł dla dowolnych polityk DLP.
      2. Instalacja polityk i reguł musi być możliwa do wykonania dla komputerów za NAT (bez VPN).
      3. System musi mieć możliwość czasowej dezaktywacji danej reguły bez jej usuwania i utraty konfiguracji.
      4. System musi mieć możliwość definiowania obiektów, na których działać będzie reguła w oparciu o parametry: nazwę komputera, adres IP, unikatowy identyfikator agenta, nazwę systemu operacyjnego, zalogowanego użytkownika, model komputera, strukturę organizacyjną, producenta komputera, dostawcę komputera, budżet z jakiego komputer został zakupiony.
      5. Nowy komputer zgłaszający się do systemu po raz pierwszy musi bez dodatkowej ingerencji administratora automatycznie pobrać oraz wdrożyć (uruchomić) przeznaczoną dla niego politykę.
      6. System musi mieć możliwość określenia ram czasowych działania danej reguły.

1. Raportowanie i eksport danych
   1. System musi umożliwiać wyeksportowanie wybranych lub wszystkich danych do formatu .xls, .xlsx, .csv, .calc (OpenOffice), .html, .mht, .xml, .jpeg, .png, .gif, .bmp.
   2. System musi umożliwiać generowanie raportów bezpośrednio z każdego widoku w aplikacji z zastosowaniem bieżących filtrów, przy czym generowanie raportu musi odbywać się po stronie serwera www.
   3. System powinien umożliwiać eksport danych z raportu do formatów: pdf, xls, doc, rtf.
   4. System musi obsługiwać raporty parametryczne z parametrami statycznymi (wprowadzanymi w momencie generowania raportów) oraz dynamicznymi (pobieranymi z bazy danych w momencie generowania raportu).
   5. System musi istnieć możliwość tworzenia i dodawania własnych raportów przez użytkownika.
2. Bezpieczeństwo
   1. System musi umożliwiać definiowanie praw dostępu dla każdego użytkownika i grup użytkowników.
   2. Kontrola dostępu musi być konfigurowana osobno dla każdego rodzaju operacji z puli: odczyt, zmiana, usunięcie, eksport.
   3. System musi umożliwiać kontrolę dostępu jednocześnie na następujących poziomie menu aplikacji, wybranych typów poleceń (dodawanie, edycja, usuwanie, przeglądanie) i struktury organizacyjnej (np. administrator A ma dostęp tylko do informacji o urządzeniach przypisanych do struktury organizacyjnej S).
   4. Uwierzytelnianie do systemu musi być realizowane:
      1. Z wykorzystaniem imiennego konta użytkownika i hasła;
      2. Z wykorzystaniem imiennego konta administratora 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.
   5. System musi udostępniać historię korzystania z poszczególnych opcji przez administratorów. W zakresie udostępnionym i objętym logowaniem.
   6. ***Przechowywanie haseł administratorów w bazie danych musi być poddane odpowiednio wysokiemu zabezpieczeniu. Hasła muszą być zapisywane jako base64 z (sól + SHA512 z login + hasło).***
   7. System musi posiadać mechanizmy automatycznego wykonywania kopii bezpieczeństwa w zadanych interwałach czasowych w formie kopii przyrostowej i nie przyrostowej oraz udostępniać informację o rezultacie wykonania kopii.
   8. System musi zapewniać pełne logowanie błędów, przechowywanie logów systemowych, logów bezpieczeństwa, logów aktywności administratorów oraz posiadać możliwość eksportu logów.
   9. System musi zapewniać mechanizmy zapewniające integralność, poufność i dostępność przechowywanych informacji.
3. Wsparcie i pomoc
   1. System musi posiadać wbudowaną dokumentację pomocy użytkownika w języku polskim oraz dokumentację w postaci filmów instruktażowych w języku polskim.
   2. Pomoc techniczna musi być świadczona w języku polskim w dni robocze w godzinach 8.00-16.00.
   3. Czas trwania usługi SLA wynosi od daty zakupu **do 30.06.2026 r.**
4. System musi wspierać następujące przykładowe zadania:
   1. Stworzenie klasyfikacji dla plików stanowiących dane istotne z punktu widzenia organizacji. Działanie: Możliwość łatwego i przejrzystego znakowania dokumentów pochodzących z wybranych aplikacji (np. aplikacji finansowo-księgowej) niewidocznymi znacznikami oraz oznaczanie dokumentów znajdujących się na serwerach plików zawierających np. umowy, porozumienia, dokumentacje projektowe.
   2. Wprowadzenie zasad dostępu do plików. Działanie: Nadanie indywidualnych uprawnień określonym grupom pracowników do wybranych operacji na plikach np. umożliwienie grupie A jedynie odczytu, grupie B odczytu i modyfikacji, a grupie C zapewnienie nieograniczonego lecz monitorowanego dostępu, gdy jednocześnie grupa A, B, C posiadają nieograniczone uprawnienia nadane polityką Active Directory.
   3. Uświadamianie pracowników o naruszeniu przez nich polityki bezpieczeństwa. Działanie: Zdefiniowanie powiadomień nadrzędnych względem aktywnych okien użytkownika informujących o rodzaju naruszonej polityki.
   4. Efektywne raportowanie stanu zabezpieczeń. Działanie: Dzięki dostępowi do konsoli zarządzającej poprzez dowolną przeglądarkę internetową (wspierającą HTML5) administrator z każdego urządzenia możne uzyskać swobodny dostęp do logów i raportów. Dzięki prowadzonej ewidencji można otrzymać statystyki osób generujących największą ilość incydentów bezpieczeństwa oraz mapę zagrożonych urządzeń i kanałów.
   5. Uniemożliwienie wypływu poza organizację ważnych danych na nośnikach zewnętrznych. Działanie: Ograniczenie możliwości przenoszenia danych na nieautoryzowane nośniki zewnętrzne, takie jak: pamięci masowe, urządzenia multimedialne.
   6. Kontrola nad bezpieczeństwem pi dostępem do sieci przewodowych i przewodowych i bezprzewodowych. Działanie: Uruchomienie polityki monitorującej podłączenia do sieci z możliwością zablokowania sieci otwartych, niezabezpieczonych, potencjalnie niebezpiecznych.