**Opis Przedmiotu Zamówienia**

**Cześć 1.** **Centralny system logów**

1. Zamawiający wymaga, aby rozwiązanie do zbierania i analizowania logów zostało dostarczone w formie rozwiązania sprzętowego i posiadało dostęp przez interfejs web umożliwiający administratorom i operatorom wykorzystanie wszystkich jego funkcji.
2. Zamawiający wymaga, aby rozwiązanie obsługiwało natywnie co najmniej urządzenia:

Check Point Spark, Check Point Harmony Endpoint, Dell iDrac, FortiMail, Microsoft SQL, Mikrotik, Synology, VMware

1. Zdarzenia z systemów Windows muszą być zbierane przez dedykowane oprogramowanie (tzw. agent) instalowane bezpośrednio na stacjach końcowych i wysyłające dane do centralnej instancji systemu.
   1. Agent Windows musi umożliwiać zbieranie logów zarówno z systemowego dziennika zdarzeń jak i z plików tekstowych w systemie Windows.
   2. Agent musi zapewniać zbieranie wszystkich danych związanych ze zdarzeniem w oryginalnej, niezmodyfikowanej formie (tzn. całość a nie tylko części zdarzenia).
2. Oferowane rozwiązanie musi umożliwiać filtrowanie zdarzeń (przykładowo odrzucanie nieistotnych) zbieranych przez agenta Windows jeszcze przed wysłaniem do centralnej instancji. Filtrowanie zdarzeń zbieranych przez agenta Windows musi być możliwe do skonfigurowania za pomocą programowania wizualnego.
3. Ilość agentów dla systemu Windows nie może być limitowana licencyjnie. Oferowane rozwiązanie musi być pozbawione limitowania pod kątem ilości zbieranych danych.
4. Wymagania wobec Agenta Windows:
   1. Dostarczenie dokumentacji opisującej proces instalacji i konfiguracji agenta.
   2. Po zainstalowaniu, nie może wymagać interwencji administratora na systemie końcowym - musi być centralnie zarządzany, a jego konfiguracja możliwa do przeprowadzenia z poziomu interfejsu graficznego web, bez konieczności ręcznego edytowania plików systemowych. Aktualizacja konfiguracji agenta musi być automatycznie dystrybuowana bezpośrednio z centralnej konsoli systemu.
   3. Musi automatycznie tłumaczyć kody zdarzeń Windows na postać tekstową wynikającą ze zdefiniowanych słowników (przykładowo: Logon Type 2 = Interactive, Logon Type 3 = Network, etc.).
   4. Musi posiadać bufor lokalny na wypadek utraty połączenia stacji końcowej z centralną instancją systemu. Dane, których nie udało się przekazać do centralnej instancji systemu, muszą zostać przekazane natychmiast po powrocie połączenia, również, gdy stacja robocza była w między czasie restartowana.
   5. Komunikacja pomiędzy agentem Windows, a centralną instancją systemu musi być zaszyfrowana (min. TLS 1.2).
   6. Musi wspierać kolekcjonowanie nie tylko podstawowych zdarzeń z dziennika zdarzeń (Application, Security, Setup, System), ale także umożliwiać zbieranie logów z folderu Applications and Services Logs. Dodatkowo agent Windows musi umożliwiać pobieranie danych logów z plików tekstowych z systemu Windows, konfigurowane z centralnej instancji systemu, w tym możliwość wybrania ich formatu danych (przykładowo: dziennik zdarzeń, plik txt, dhcp, iis).
   7. Musi automatycznie dodawać opis tekstowy do wszystkich zbieranych zdarzeń, dokładnie tak jak jest to prezentowane w Dzienniku Zdarzeń systemu Windows.
   8. Musi umożliwiać zbieranie logów z płaskich plików w systemie, z którego zbierane są logi poprzez podanie ich ścieżki w systemie plików w menu konfiguracji agenta. Konfiguracja ścieżki musi uwzględniać wykorzystanie tzw. wildcardów (przykładowo: C\Windows\System32\dhcp\logs\Dhcp\*.log - pobranie wszystkich plików z wskazanego folderu zaczynających się od "Dhcp" i kończących na ".log").
   9. Musi automatycznie odpytywać centralny system w zadanym interwale - tzw. heartbeat - w celu sprawdzenia czy zaszły zmiany w konfiguracji - jeżeli tak, to agent pobiera nową konfigurację, a następnie ją implementuje. Nie jest dopuszczalne "wypychanie" konfiguracji z centralnego systemu do agenta.
5. Interfejs graficzny web umożliwiający dostęp do logów, tworzenia alertów i parserów, raportów oraz zarządzania systemem musi być jednolity oraz zunifikowanym tak aby wszystkie operacje konfiguracji, zarządzania i analizy logów były w nim wykonywane.
6. Nie dopuszcza się stosowania wielu różnych interfejsów. Interfejs ten musi być dostępny z poziomu popularnych przeglądarek (przykładowo: Google Chrome, Mozilla Firefox, Opera, Microsoft Edge).
7. Stosowany w rozwiązaniu interfejs graficzny musi umożliwiać łatwe klasyfikowanie danych wejściowych (logów) na potrzeby dalszego procesowania. Klasyfikowanie powinno umożliwiać przypisywanie określonych logów do odpowiednich parserów oraz nadawanie im tagów ułatwiających dalszą pracę z logami (np. wyszukiwanie). Logika klasyfikacji powinna być tworzona przy wykorzystaniu tzw. programowania wizualnego.
8. Oferowane rozwiązanie musi umożliwiać rozbudowywanie natywnie dostępnych funkcjonalności, takich jak klasyfikacja, parsowanie, alertowanie oraz filtrowanie poprzez tak zwane programowanie wizualne, które polega na tworzeniu kodu z graficznych bloków reprezentujących określone instrukcje i funkcje na zasadach WYSIWYG.
9. Zamawiający wymaga, aby programowanie wizualne było możliwe do wykonania przez osoby posiadające podstawową wiedzę programistyczną taką jak znajomość min. instrukcji warunkowych, pętli czy zmiennych, jednakże rozwiązanie musi posiadać możliwość testowania i weryfikowania poprawności logiki stworzonego kodu.
10. Oferowane rozwiązanie musi udostępniać pre-definiowane widoki danych (dashboards) podzielone na kategorie pod względem typu lub producenta urządzenia źródłowego lub aplikacji.
11. Wraz z każdą nową wersją oprogramowania zapisane widoki muszą być automatycznie aktualizowane.
12. Wymagania ogólne wobec rozwiązania:
    1. Filtrowanie nieistotnych zdarzeń na etapie klasyfikacji. Logika filtrowania powinna być tworzona przy wykorzystaniu tzw. programowania wizualnego. Wymagane jest dostarczenie dokumentacji opisującej ten proces.
    2. Zapis oryginalnej wersji odbieranych logów.
    3. Proste wyszukiwanie zapisanych w bazie logów i tworzenie raportów w formie graficznej bez konieczności wykorzystania dedykowanego języka programowania lub zapytań SQL. Wyszukiwanie i raporty muszą być integralną częścią oferowanego rozwiązania i muszą być dostępne przez interfejs graficzny web.
    4. Nie dopuszcza się możliwości modyfikacji bądź manualnego usunięcia logów zapisanych w bazie. Każdy log musi posiadać unikalny identyfikator, który umożliwi jego jednoznaczne rozróżnienie.
    5. Prezentowanie logów ma być realizowane w formie wykresów, zgrupowanych w tzw. widokach (dashboard). Widoki muszą być dynamicznie aktualizowane i interaktywne (tzw. "drill down" - przykładowo: wybranie wartości przedstawionej na jednym wykresie powoduje automatyczne utworzenie filtru wyszukiwania w oparciu o wybraną wartość i dostosowanie pozostałych wykresów).
    6. Tworzenie własnych parserów logów przy wykorzystaniu programowania wizualnego z poziomu interfejsu graficznego web. Wymagane jest dostarczenie dokumentacji zawierającej czytelną instrukcję tworzenia parserów.
    7. Odbieranie wszystkich rodzajów logów. W przypadku braku odpowiedniego parsera dla odbieranego logu, system powinien zapisać go w bazie danych w formie źródłowej (RAW) i umożliwić jego wyszukiwanie.
    8. Automatyczne wzbogacanie logi o tzw. metadane, czyli informacje opisujące dany log (przykładowo: typ źródła, protokół transportowy, port docelowy, tagi, nagłówek syslog) i możliwość wyszukiwania wszystkich zapisanych logów w oparciu o te dane. Metadane powinny być dodawane do logu automatycznie nawet jeżeli nie został on poddany parsowaniu.
    9. Musi posiadać wsparcie dla oprogramowania Elastic Beats - innymi słowy system musi umożliwiać zbieranie logów wysyłanych przez agenty Beats (filebeat/winlogbeat/auditbeat/metricbeat itd.).
13. W zakresie parsowania musi być możliwość:
    1. Tworzenia lub modyfikacji parsera - musi istnieć możliwość weryfikacji poprawności utworzonej logiki poprzez zastosowanie jej do przykładowego logu i wyświetlenie ostatecznej wersji w jakiej log zostanie zapisany w bazie, jeżeli testowany parser zostanie użyty. W przypadku wystąpienia błędów w logice parsera, system powinien poinformować o tym użytkownika.
    2. W procesie parsowania oferowane rozwiązanie musi normalizować odbierane logi do ujednoliconego formatu poprzez przypisanie poszczególnych wartości logu do odpowiadających im kluczy (format klucz = wartość). Każdy z utworzonych w procesie parsowania kluczy powinien być oddzielnie indeksowany w bazie danych, aby umożliwić szybkie wyszukiwanie wartości skojarzonych z danym kluczem. Zintegrowane w systemie parsery powinny automatycznie wzbogacać procesowane logi o odpowiednią kategorię. Wymagane jest rozróżnianie przynajmniej następujących typów logów: udane logowanie, nieudane logowanie, wylogowanie, zmiana konfiguracji.
    3. Dodania w/w kategorii podczas tworzenia własnych parserów.
    4. Zamiany wybranych elementów logu na podstawowe typy (integer, float), w celu wykonywania na nich operacji matematycznych (suma, średnia, największa/najmniejsza wartość etc.) podczas prezentowania ich na dashboardach.
    5. Wykorzystania operacji matematycznych (dodawanie, odejmowanie, mnożenie, dzielenie) oraz operacji natywnego kodowania/dekodowania URL. Te operacje muszą umożliwiać tworzenie logiki mającej na celu tworzenie linków URL do zewnętrznych systemów oraz połączenie narzędzia z zewnętrznymi aplikacjami.
    6. Dodawania własnych znaczników czasu do odbieranych logów i wykorzystywać go podczas przeglądania danych. Jednocześnie system musi zachowywać oryginalny znacznik czasu z odebranych logów.
    7. Tworzenie własnych parserów musi umożliwiać ustawienie typu wartości jako adres MAC i identyfikację producenta urządzenia sieciowego.
    8. Automatycznego wzbogacania wartości IP wyekstraktowane z pól logu o powiązany rekord DNS i dane GeoIP, aby umożliwić ich graficzną reprezentację na widoku mapy świata bez konieczności wykorzystania zewnętrznych usług bądź aplikacji.
    9. Średnią stałą wydajność procesowania min. 2000 EPS (logów na sekundę), przy założeniu średniego rozmiaru logu równego 700 Bajtów. W przypadku wystąpienia większej chwilowej ilości logów na sekundę, rozwiązanie musi być w stanie wykorzystać bufor i umożliwić odbieranie dwukrotnej większej wartości prze co najmniej 5 minut.
14. Oferowane rozwiązanie musi umożliwiać również:
    1. Zbieranie logów i zdarzeń z systemów Windows poprzez dedykowanego agenta instalowanego na stacji końcowej/serwerze. Agent musi być centralnie zarządzany z konsoli systemu.
    2. Odbieranie logów na przynajmniej 50 różnych portach UDP/TCP w celu ułatwienia rozróżnienia źródeł.
    3. Procesowanie (kolekcjonowanie oraz parsowanie) logów z dowolnych źródeł takich jak aplikacje, systemy operacyjne oraz urządzenia sieciowe.
    4. Zbieranie logów z platformy Office365 bez konieczności instalacji dodatkowych komponentów. Proszę dostarczyć dokumentację opisującą proces konfiguracji connectora Office365.
    5. Monitorowanie źródeł logów i tworzenie reguł mających na celu powiadamianie administratora systemu w przypadku, w którym źródło logów zdefiniowane w regule nie wyśle logów w określonym interwale. System musi być dostarczony wraz z parserami do obsługi logów generowanych przez urządzenia najpopularniejszych dostawców rozwiązań IT oraz umożliwiać tworzenie własnej logiki parsowania dla nietypowych źródeł.
    6. Odbieranie i procesowanie logów, zdarzeń oraz innych danych przesyłanych przez urządzenia w sposób jawny i ustandaryzowany, wykorzystując co najmniej następujące protokoły: UDP/TCP SYSLOG, TCP RELP (nieszyfrowany), TCP RELP (szyfrowany).
    7. Łatwe tworzenie ról definiujących poziom dostępu użytkowników do zapisanych logów oraz poszczególnych elementów systemu. Wymagane jest dostarczenie dokumentacji opisującej sposób tworzenia ról użytkowników.
    8. Wzbogacanie logów o dodatkowe informacje z zewnętrznych list (przykład: wzbogacenie nazwy użytkownika o jego adres email i przynależność do grup AD).
    9. Integrację z systemem LDAP w celu logowania użytkowników. W przypadku awarii systemu LDAP, Zamawiający wymaga również możliwości logowania lokalnego.
    10. Tagowanie indywidualnych źródeł danych, aplikacji, urządzeń czy całych podsieci IP, w celu oznaczania, przykładowo: lokalizacji urządzenia, jego typu, krytyczności etc. Tagi muszą być możliwe do dodania w procesie tworzenia parsera. Wszystkie dodane tagi muszą być przechowywane razem z logiem zapisanym w bazie. System musi umożliwiać filtrowanie i wyszukiwanie logów w oparciu o tagi, a także umożliwiać ograniczenie widoczności logów posiadających określony tag w procesie definiowania ról.
    11. Wykorzystanie REST-API do integracji z zewnętrznymi systemami do monitoringu (Zabbix, Nagios, MRTG etc.).
    12. Integrację z bazami danych (przynajmniej: MSSQL, MySQL, Oracle i PostgreSQL) poprzez konektor ODBC (integracja rozumiana jako możliwości pobierania całych wierszy wybranych tabel w bazie).
    13. Integrację z platformą wirtualizacji Vmware (ESXi, vSphere) poprzez dedykowany konektor pobierający logi i zdarzenia bezpośrednio z platformy.
    14. Weryfikację poprawności działania własnych parserów w trakcie ich pisania.
    15. Zbieranie danych przynajmniej w formatach RAW, Syslog RFC5424, CEF, LEEF, JSON RFC8259.
    16. Wspieranie podstawowych funkcji SIEM - tworzenie tzw. korelacji zdarzeń, umożliwiających wygenerowanie alertu w przypadku przekroczenia określonego limitu lub wystąpienia kilku zdarzeń w zdefiniowanym oknie czasowym. Tworzenie i edycja reguł korelacji musi być możliwa do przeprowadzenia za pomocą interfejsu programowania graficznego wyposażonego w funkcjonalność sprawdzania działania logiki reguły na przykładowych logach.
    17. Wdrożenie w trybie wysokiej dostępności, w którym możliwe jest klastrowanie przynajmniej 2 urządzeń. Ustawienia klastra muszą być możliwe do skonfigurowania przez interfejs graficzny web, nie jest dopuszczalne konfigurowanie klastra poprzez ręczne modyfikowanie plików systemu operacyjnego. System musi dostarczać użytkownikom czytelnych informacji o stanie klastra i synchronizacji bazy. Wymaga się dostarczenia dokumentacji opisującej cały proces tworzenia klastra oraz odzyskiwania danych w przypadku awarii jednego z komponentów klastra. Urządzenia pracujące w klastrze muszą przyśpieszać wyszukiwanie poprzez równoległe współdzielenie obciążenia.
    18. Generowanie alertów, jeżeli w procesowanym logu zostaną spełnione zdefiniowane warunki. Alert musi być możliwy do wysłania poprzez wiadomość e-mail, a jego treść możliwa do utworzenia przez użytkownika. Oferowane rozwiązanie musi być również wyposażone w alerty i korelacje utworzone przez producenta.
    19. Wykorzystanie pól procesowanego logu do tworzenia treści wiadomość e-mail.
    20. Umożliwiać tworzenie alertów i korelacji poprzez wykorzystanie programowania wizualnego. Podobnie jak w przypadku tworzenia parserów, musi istnieć możliwość weryfikacji poprawności utworzonej logiki poprzez wykorzystanie testowego logu w oknie tworzenia alertu oraz powiadamiania o ewentualnych błędach. Wymagane jest dostarczenie dokumentacji opisującej proces tworzenia i testowania poprawności alertu.
    21. Wysłanie logu naruszającego zdefiniowaną logikę alertu do zewnętrznych systemów, co najmniej za pomocą protokołu SMPT lub Syslog (TCP). System musi umożliwiać definiowanie własnego formatu przesyłanego logu w celu łatwiejszego dostosowania go (integracji) do systemu docelowego.
    22. Nadawanie alertom nowych tagów.
    23. Wspierać tworzenie i odzyskiwanie kopii zapasowej konfiguracji.
    24. Tworzenie i odzyskiwanie kopii zapasowej bazy danych. Tworzenie kopii zapasowej musi być możliwe zarówno na żądanie jak i w określonych interwałach czasowych. Tworzenie i odzyskiwanie musi być możliwe do wykonania z poziomu interfejsu graficznego web, bez konieczności tworzenia/modyfikowania skryptów, makr lub plików systemu operacyjnego.
    25. Oferowane rozwiązanie musi być dostarczone w formie urządzenia fizycznego spełniającego następujące wymagania:
    26. Obudowa - rozmiar max 2U, wyposażone w ramię do kabli umożliwiające wysunięcie urządzenia z szafy rack na potrzeby serwisowe bez konieczności wyłączania. Wentylatory urządzenia muszą być wymienialne w trakcie pracy urządzenia i być redundantne skierowane ruchem przepływu powietrza front -> tył.
    27. Interfejsy sieciowe - minimum 4 porty 1Gbit LAN + 1 dedykowany 1Gbit porty do zarządzania sprzętem. Konfiguracja parametrów wszystkich interfejsów sieciowych (w tym LACP) musi odbywać się z interfejsu graficznego web oraz musi być szczegółowo opisana w dokumentacji.
    28. Zasilanie - urządzenie musi być wyposażone w 2 źródła zasilania z redundancją 1+1.
    29. Przestrzeń dyskowa - wspierana przez sprzętowy akcelerator SAS RAID-5. Kontroler macierzy dyskowej musi być wyposażony w zapasową baterię lub pamięć flash. Minimum 4 dyski edycji RAID do wykorzystania w warunkach data center. Redundancja dysków nie może wpływać na wymaganą minimalną przestrzeń dyskową. Wymagana przestrzeń składowania danych o rozmiarze przynamniej M - 12 TB oraz wspierać kompresję przechowywanych danych.
    30. System operacyjny - zamknięty przez producenta bez możliwości połączeń SSH. Aktualizowany z konsoli administracyjnej poprzez protokół https (wszystkie elementy systemu muszą być ustawialne z interfejsu graficznego web, bez konieczności edytowania żadnych plików systemowych, skrytpów lub makr).
    31. Virtual KVM (keyboard, video, mouse) – urządzenie musi posiadać możliwość zdalnego zarządzania oraz być dostarczone z licencją odpowiedniego typu (iLO, iDRAC etc).
15. Zamawiający wymaga, aby oferowane rozwiązanie gwarantowało przechowywanie danych w okresie oczekiwanej retencji, aby dane były dostępne do przeszukiwania natychmiastowo, bez wprowadzania opóźnienia w postaci importu z zewnętrznych baz danych.
16. W przypadku przeciążenia systemu logi nie mogą być tracone. Wszystkie nieobsłużone logi muszą być buforowane, a administrator systemu powiadamiany w momencie, w którym bufor zacznie się zapełniać. Bufor nie może być mniejszy nić 50GB.
17. Oferent musi dostarczyć kompletną dokumentację – instrukcję obsługi oferowanego rozwiązania. Wymagane jest dostarczenie broszury szczegółowo przedstawiającej parametry techniczne oferowanego systemu. Wymaga się dostarczenia dokumentacji w formie elektronicznej lub linku do jej wersji online na stronach producenta. Nie dopuszcza się dokumentacji odnoszącej się z/do źródeł zewnętrznych, innych niż producenta. Dokumenty te, tj. instrukcję obsługi oraz broszury
18. Zamawiający wymaga możliwości aktualizacji systemu dystrybuowanej w formie pojedynczego pliku i instalowane za pośrednictwem interfejsu graficznego web. Wszystkie aktualizacje muszą być możliwe do zainstalowania bez wsparcia dostawcy/producenta.
19. Wymagamy dostarczenia przynajmniej 4 ostatnich dokumentów release notes w celu zweryfikowania proponowanych parametrów systemu. System musi umożliwiać cofnięcie do poprzedniej wersji oprogramowania w przypadku wystąpienia problemów z działaniem po aktualizacji. Operacja musi być możliwa do wykonania bez wsparcia dostawcy/producenta.
20. Ilość urządzeń z których zbierane są dane oraz ilość logów liczona w GB/dzień nie może być ograniczona licencyjnie.
21. Wymagane wsparcie na oprogramowanie - minimum 1 rok / max. 5 lat.
22. Dostarczone rozwiązanie musi zostać dostarczone na koszt wykonawcy oraz uruchomione, a personel referatu IT Urzędu Miejskiego w Sędziszowie musi zostać przeszkolony z jego obsługi. Podczas szkolenia wymaga się uruchomienia co najmniej:
23. 5 źródeł z systemów Microsoft Windows, przykładowo:
    * Serwer MS SQL
    * Serwer Exchange
    * Serwer DHCP
24. 10 źródeł urządzeń przekazujących logi poprzez syslog UDP 514.
    * np.: UniFi, Dell iDrac, Linux, Mikrotik, PostgreSQL, Synology NAS…
25. Mechanizm przekazywania logów o stanie alarmowym do innego systemu w formacie syslog.
26. Wykonawca musi zapewnić pierwszą linię wsparcia w języku polskim trybie 8x5. W celu realizacji wymogu wymagane jest posiadanie certyfikatów ISO 9001, ISO 27001 i ISO 22301 w zakresie serwisowania urządzeń informatycznych.

**Cześć 2. System zaawansowanego backupu**

1. **Deduplikator sprzętowy – min. wymagania:**

|  |  |
| --- | --- |
| **Lp.** | **Opis parametrów urządzenia** |
| 1. | Urządzenie jest przeznaczone do deduplikacji i przechowywania kopii zapasowych.  Urządzenie posiada parametry wyspecyfikowane w niniejszej tabeli. |
| 2. | Oferowane urządzenie oferuje przestrzeń min. 24TB netto (powierzchni użytkowej) bez uwzględniania mechanizmów protekcji – przestrzeń dedykowana do gromadzenia deduplikatów, zapewnia skalowalność do 250TB netto (powierzchni użytkowej widocznej po założeniu systemu plików) |
| 3. | Urządzenie pozwala na rozbudowę o warstwę typu CLOUD dedykowaną do długotrwałego przechowywania danych (tzw. Long Term Retention) – dane o określonej retencji (zgodnie z założoną polityka retencyjną), bez pośrednictwa dodatkowych urządzeń (typu GATEWAY) powinny zostać przemigrowane (w postaci zdeduplikowanej) na dodatkową warstwę, zapewnione jest wsparcie dla dla AWS, Microsoft Azure oraz Google GCP. Możliwa jest enkrypcja danych przechowywanych na warstwie typu Cloud. Urządzenie posiada licencję  na przestrzeń 80TB netto dla warstwy CLOUD. |
| 4. | Oferowane urządzenie posiada min.:   * 4 porty Eth 10 Gb/s Base-T   Urządzenie można rozbudować o dodatkowe porty ethernet:   * 4 porty 10/25Gb/s Eth   Na każdym z w/w portów istnieje możliwość obsługi protokołów CIFS, NFS, z deduplikacją na źródle  Urządzenie można rozbudować o dodatkowe porty Fiber Channel:   * 4 porty FC 32Gb/s   Istnieje możliwość obsługi poprzez porty FC protokołów VTL oraz deduplikacji na źródle (możliwość dodania dwóch portów FC oznacza oficjalnie wsparcie takiej konfiguracji przez producenta urządzenia, wolny slot na dodatkową kartę HBA w przypadku oferowanej konfiguracji urządzenia oraz możliwość natychmiastowego zamówienia u producenta odpowiedniej karty rozszerzeń) |
| 5. | Oferowane urządzenie umożliwia jednoczesny dostęp wszystkimi poniższymi protokołami:   * CIFS, NFS * zapewniając deduplikację na źródle, posiada wsparcie dla aplikacji Commvault (na poziomie Media Server, a także Client Direct przy użyciu storage accelerator), Veeam Backup and Replication (na poziomie Veeam Data Mover), NetWorker na poziomie standardowego klienta * VTL (min. 10 jednocześnie) |
| 6. | Urządzenie posiada licencje pozwalające na jednoczesną obsługę protokołów CIFS, NFS,  deduplikacji na źródle, VTL do oferowanej pojemności urządzenia |
| 7. | Oferowane pojedyncze urządzenie osiąga zagregowaną wydajność (dla maksymalnej konfiguracji) protokołami: **NFS** co najmniej 10 TB/h (dane podawane przez producenta) oraz co najmniej 20 TB/h z wykorzystaniem **deduplikacji na źródle** (dane podawane przez producenta). |
| 8. | Urządzenie pozwala na jednoczesną obsługę min. 250 strumieni w tym jednocześnie:   * zapis danych 150 strumieniami * odczyt danych 50 strumieniami * replikacja 50 strumieniami   pochodzących z różnych aplikacji oraz dowolnych protokołów (CIFS, NFS, VTL, deduplikacja  na źródle) oraz dowolnych interfejsów (FC, LAN) w tym samym czasie.  Wymienione wartości 250 jednoczesnych strumieni dla wszystkich protokołów (czyli jednocześnie 150 dla zapisu i jednocześnie 50 strumieni dla odczytu i jednocześnie 50 strumieni dla replikacji) mieści się w przedziale oficjalnie rekomendowanym i wspieranym przez producenta urządzenia.  Wszystkie zapisywane strumienie podlegają globalnej deduplikacji przed zapisem na dysk (in-line) jak opisano w min. wymaganiach. |
| 9. | Oferowane urządzenie posiada możliwość emulacji następujących bibliotek taśmowych:   * StorageTek L180 * IBM TS 3500 |
| 10. | Oferowane urządzenie ma możliwość emulacji napędów taśmowych LTO5 oraz LTO7 |
| 11. | Urządzenie min. umożliwia (w przypadku VTL’a) emulację 250 napędów, emulację 30 000 slotów w przypadku poj. biblioteki taśmowej oraz emulację sumarycznie 60 000 slotów. |
| 12. | Oferowane urządzenie deduplikuje dane in-line przed zapisem na nośnik dyskowy. Na wewnętrznych dyskach urządzenia nie są zapisywane dane w oryginalnej postaci (niezdeduplikowanej) z jakiegokolwiek fragmentu strumienia danych przychodzącego do  urządzenia. |
| 13. | Technologia deduplikacji wykorzystuje algorytm bazujący na zmiennym, dynamicznym bloku jednak o wielkości nie większej niż 12 kB.  Algorytm samoczynnie i automatycznie dopasowuje się do otrzymywanego strumienia danych co oznacza, że urządzenie dzieli otrzymany pojedynczy strumień danych na bloki o różnej długości, bez konieczności podejmowania czynności mających na celu ustalenie predefiniowanej długości bloków używanych do deduplikacji danych określonego typu. Deduplikacja zmiennym, dynamicznym blokiem oznacza, że wielkość każdego bloku (na jaki są dzielone dane pojedynczego strumienia backupowego) jest inna niż poprzedniego oraz jest indywidualnie ustalana przez algorytm deduplikacji zastosowany w urządzeniu, oferowane urządzenie nie dzieli jakiegokolwiek pojedynczego strumienia danych backupowych na bloki o ustalonej, tej samej długości. |
| 14. | Oferowany produkt musi posiadać obsługę mechanizmów globalnej deduplikacji dla danych otrzymywanych jednocześnie wszystkimi protokołami (CIFS, NFS, VTL, deduplikacja na źródle) przechowywanych w obrębie całego urządzenia co oznacza, że przechowywany na urządzeniu fragment danych nie jest ponownie zapisany bez względu na to, jakim protokołem zostanie ponownie otrzymany. Wszystkie emulowane jednocześnie w obrębie urządzenia biblioteki wirtualne (VTL) oraz udziały NFS/CIFS również podlegają globalnej deduplikacji – blok danych otrzymany i zapisany w wirtualnej bibliotece „A”, nie zostaje ponownie zapisany jeśli trafi do innej wirtualnej biblioteki „B” w obrębie tego samego urządzenia (to samo dotyczy udziałów NFS/CIFS). Przestrzeń składowania zdeduplikowanych danych jest jedna dla wszystkich protokołów dostępowych, co oznacza zastosowanie pojedynczej bazy deduplikatów bez względu na ilość/rodzaj używanych jednocześnie protokołów dostępowych. |
| 15. | Proces deduplikacji odbywa się in-line – w pamięci urządzenia, przed zapisem danych na nośnik dyskowy. Zapisowi na system dyskowy muszą podlegać tylko unikalne bloki danych nie zapisane jeszcze na system dyskowy urządzenia. Dotyczy to każdego fragmentu przychodzących do urządzenia danych. Nie jest to zapewnione, jeżeli deduplikacja in-line realizowana będzie przez zewnętrzną aplikację backup’ową. Deduplikacja in-line dotyczy zapisu danych przez każdy z interfejsów, w przypadku: NFS, CIFS oraz VTL realizacja deduplikacji in-line nie jest w żadnym stopniu zależna od konkretnej aplikacji backu’owej, dane zapisywane poprzez interfejsy: NFS, CIFS bez użycia jakiejkolwiek aplikacji backup’owej również są deduplikowane w sposób in-line |
| 16. | Proponowane rozwiązanie w żadnej fazie nie korzysta (w całości lub częściowo) z bufora na składowanie danych w postaci oryginalnej (niezdeduplikowanej) w celu ich późniejszej deduplikacji (deduplikacja in-line) |
| 17. | Wszystkie unikalne bloki przed zapisaniem na dysk są dodatkowo kompresowane. |
| 18. | Tryb zapisu zabezpieczanych danych nie umożliwia nadpisywania danych, dane mogą być zapisywane jedynie w trybie append-only, dane dla których wygasła retencja powinny zostać usunięte podczas procesu czyszczenia tzw. Cleaning, dotyczy to wszystkich danych zapisanych na urządzeniu a nie wybranych grup danych objętych działaniem blokad  zabezpieczających przed usunięciem/modyfikacją danych. |
| 19. | Oferowane urządzenie wspiera (zapewnione jest formalne wsparcie producenta urządzenia), następujące aplikacje: Commvault, Veeam Backup and Replication, NetWorker. W przypadku współpracy z każdą z poniższych aplikacji:   * Commvault * Veeam Backup and Replication * NetWorker   urządzenie umożliwia deduplikację na źródle (w przypadku Commvault: na poziomie Media Server a także Client Direct przy użyciu storage accelerator, w przypadku Veeam Backup and Replication na poziomie Veeam Data Mover), w przypadku NetWorker na poziomie standardowego klienta) i przesłanie nowych, nie znajdujących się jeszcze na urządzeniu bloków poprzez sieć LAN.  Deduplikacja w wyżej wymienionych przypadkach zapewnia, że do oferowanego urządzenia są transmitowane poprzez sieć LAN jedynie fragmenty danych nie znajdujące się dotychczas na urządzeniu. |
| 20. | W przypadku przyjmowania backupów z Commvault, Veeam Backup and Replication, NetWorker, urządzenie umożliwia deduplikację na źródle (na poziomie Media Server dla CommVault, Data Mover dla Veeam, klienta dla NetWorker) i przesłanie nowych, nieznajdujących się jeszcze na urządzeniu bloków poprzez sieć FC.  Deduplikacja w wyżej wymienionych przypadkach zapewnia, że do oferowanego urządzenia  są transmitowane poprzez sieć FC jedynie fragmenty danych nie znajdujące się dotychczas na urządzeniu. |
| 21. | Oferowane urządzenie umożliwia uruchamianie maszyn wirtualnych VMware bezpośrednio  z danych backupowych bez konieczności odtwarzania danych. |
| 22. | Posiada funkcjonalność Load Balancing oraz Link Failover w obrębie portów (Eth)  wykorzystywanych przez aplikację backupową. |
| 23. | Posiada wsparcie dla backupów typu Virtual Synthetics w przypadku aplikacji Commvault,  Veeam Backup and Replication oraz NetWorker. |
| 24. | W przypadku deduplikacji na źródle poprzez sieć IP (LAN oraz WAN), urządzenie posiada możliwość szyfrowania komunikacji kluczem minimum 256 bitów. |
| 25. | Urządzenie umożliwia zaszyfrowanie przechowywanych danych, posiada licencje  umożliwiające zaszyfrowanie i przechowywanie zaszyfrowanych danych w obrębie maksymalnej pojemności oferowanego urządzenia. |
| 26. | Urządzenie wspiera deduplikację na źródle poprzez sieć FC (SAN) minimum dla  następujących systemów operacyjnych:   * Windows * Linux (RedHat, SuSE) |
| 27. | Oferowane urządzenie umożliwia bezpośrednią replikację danych do drugiego urządzenia  takiego samego typu. Konfiguracja replikacji jest możliwa w każdym z trybów:   * jeden do jednego * wiele do jednego * jeden do wielu * kaskadowej (urządzenie A replikuje dane do urządznia B, które te same dane replikuje do urządzenia C).   Replikacja odbywa się w trybie asynchronicznym. Transmitowane mogą być tylko te  fragmenty danych (bloki), które nie znajdują się na docelowym urządzeniu. Ewentualna licencja na replikację jest przedmiotem postępowania. |
| 28. | Urządzenie umożliwia wydzielenie określonych portów Ethernet dedykowanych do  replikacji. |
| 29. | W przypadku wykorzystania portów Ethernet do replikacji urządzenie umożliwia  przyjmowanie backupów, odtwarzanie danych, przyjmowanie strumienia replikacji, wysyłanie strumienia replikacji tymi samymi portami. |
| 30. | W przypadku replikacji danych między dwoma urządzeniami, urządzenie integruje się  z aplikacjami Commvault oraz NetWorker i pozwala na realizację funkcjonalności:   * replikacja odbywa się bezpośrednio między dwoma urządzeniami bez udziału serwerów pośredniczących * replikacji podlegają tylko te fragmenty danych (na poziomie bloków używanych do   deduplikacji), które nie znajdują się na docelowym urządzeniu   * replikacja zarządzana jest z poziomu aplikacji   aplikacja posiada informację o obydwu kopiach zapasowych znajdujących się w obydwu urządzeniach bez konieczności przeprowadzania procesu inwentaryzacji |
| 31. | Oferowane urządzenie działa poprawnie przy zapełnieniu danymi na poziomie 90%.  Dokumentacja urządzenia nie wskazuje na ew. problemy, obostrzenia, które są efektem zapełnienia urządzenia zabezpieczanymi danymi, na poziomie mniejszym niż 90%. |
| 32. | Zapewniona jest możliwość ograniczenia pasma używanego do replikacji między dwoma urządzeniami – oferowane urządzenie jest wyposażone w mechanizm umożliwiający zarządzaniem stopnia wykorzystania pasma na potrzeby replikacji. |
| 33. | Zdeduplikowane i skompresowane dane przechowywane w obrębie podsystemu dyskowego  urządzenia są chronione za pomocą technologii RAID 6 bądź równoważnej. |
| 34. | Oferowane urządzenie pozwala na realizację oraz przechowywanie SnapShot’ów, czyli umożliwia zamrożenie obrazu danych (stanu backupów) w urządzeniu na określoną chwilę. Oferowane urządzenie umożliwia również odtworzenie danych ze Snapshot’u.  Odtworzenie danych ze Snapshot’u nie wymaga konieczności nadpisania danych produkcyjnych jak również nie oznacza przerwy w normalnej pracy urządzenia  (przyjmowania/odtwarzania backupów). |
| 35. | Urządzenie pozwala na przechowywanie 500 Snapshotów jednocześnie w obrębie  oferowanej przestrzeni, przy zachowaniu globalnej deduplikacji oraz standardowego trybu  pracy urządzenia – umożliwiającego wykorzystanie wszystkich dostępnych funkcjonalności. |
| 36. | Urządzenie umożliwia podział na logiczne części. Dane znajdujące się w każdej logicznej  części są między sobą deduplikowane (globalna deduplikacja między logicznymi częściami urządzenia). |
| 37. | Urządzenie posiada możliwość podziału na 10 logicznych części pracujących równolegle.  Producent oficjalnie wspiera pracę 10 logicznych części pracujących równolegle z pełną  wydajnością urządzenia. |
| 38. | Dla każdej z w/w logicznych części oferowanego urządzenia jest możliwość zdefiniowania oddzielnego użytkownika zarządzającego daną logiczną częścią deduplikatora. Użytkownicy zarządzający logiczną częścią A widzą tylko i wyłącznie zasoby logicznej części A i nie mogą widzieć żadnych innych zasobów oferowanego urządzenia. |
| 39. | Zapewniona jest możliwość zaprezentowania każdej z logicznych części oferowanego urządzenia, jako niezależnego urządzenia dostępnego za pośrednictwem:   * CIFS * NFS * VTL |
| 40. | Urządzenie umożliwia zdefiniowanie blokady skasowania danych (funkcjonalność WORM). Blokada skasowania danych chroni plik w zdefiniowanym czasie przed usunięciem pliku, modyfikacją pliku.  Blokada skasowania danych działa w dwóch trybach (do wyboru przez administratora):   1. Możliwość zdjęcia blokady przed upływem ważności danych 2. Brak możliwości zdjęcia blokady przed upływem ważności danych (COMPLIANCE), w tym wypadku wspierane są normy SEC 17a-4(f) oraz ISO Standard 15489-1 w zakresie ochrony danych, zapewnione jest oficjalne wsparcie wymaganej blokady przez aplikację Commvault, Veeam Backup and Replication oraz NetWorker.   Licencje na blokadę usunięcia/zmiany przechowywanych plików są dostarczone wraz z urządzeniem.  Istnieje możliwość automatycznego uruchamiania blokady (podczas zapisu) WORM dla danych zapisywanych na obszar objęty działaniem wspomnianej blokady. W każdym przypadku zapewniona jest również możliwość używania blokady WORM dla obrazu danych uzyskanych poprzez użycie funkcjonalności SnapShot. |
| 41. | Urządzenie ma możliwość przechowywania danych niezmienialnych:   * Video * Grafika * Nagrania dźwiękowe * Pliki pdf   na udziałach CIFS/NFS. |
| 42. | Urządzenie weryfikuje dane po zapisie (nie chodzi o ew. weryfikację danych indeksowych generowanych przez urządzenie, ale o weryfikację wszystkich zabezpieczanych danych backup’owych). Każda zapisana na dyskach porcja danych jest odczytana i porównana z  danymi otrzymanymi przez urządzenie. Powyższa weryfikacja jest realizowana w locie, czyli przed usunięciem z pamięci oryginalnych danych (otrzymanych z aplikacji backupowej), jest realizowana w trybie ciągłym (a nie ad-hoc), parametry wydajnościowe urządzenia uwzględniają tę funkcjonalność.  W oficjalnej dokumentacji producenta oferowanego urządzenia istnieje potwierdzenie  opisanej funkcjonalności. |
| 43. | Urządzenie automatycznie usuwa przeterminowane dane (bloki danych nie należące do  backupów o aktualnej retencji) w procesie czyszczenia. |
| 44. | Proces usuwania przeterminowanych danych (czyszczenia) nie uniemożliwia pracy procesów  backupu / odtwarzania danych (zapisu / odczytu danych z zewnątrz do systemu). |
| 45. | Istnieje możliwość zdefiniowania maksymalnego obciążenia urządzenia procesem usuwania przeterminowanych danych (poziomu obciążenia procesora), co jest potwierdzone w ogólnodostępnej dokumentacji. |
| 46. | Istnieje możliwość zdefiniowania harmonogramu wg. którego wykonywany jest proces  usuwania przeterminowanych danych (czyszczenia), realizowany równolegle z procesami backup/restore/replication. |
| 47. | Standardowa częstotliwość usuwania przeterminowanych danych (czyszczenie) nie jest większa niż 1 raz na tydzień - minimalizując czas, w którym backupy/odtworzenia narażone są na spowolnienie (co jest potwierdzone na podstawie dokumentacji typu DOBRE PRAKTYKI  publikowanej przez producenta). |
| 48. | Urządzenie umożliwia systemowo (wbudowana funkcjonalność) - realizację procesu  pierwszego czyszczenia dopiero po przekroczeniu 75% zajętości oferowanej przestrzeni. |
| 49. | Urządzenie ma możliwość zarządzania poprzez   * Interfejs graficzny dostępny z przeglądarki internetowej * Poprzez linię komend (CLI) dostępną z poziomu ssh (secure shell) |
| 50. | Oprogramowanie do zarządzania rezyduje na oferowanym urządzeniu deduplikacyjnym. |
| 51. | Oferowane urządzenie ma możliwość sprawdzenia pakietu upgrade’ującego firmware  urządzenia (GUI lub CLI), to znaczy sprawdzenia czy nowa wersja systemu nie spowoduje  problemów z urządzeniem. |
| 52. | Urządzenie jest rozwiązaniem kompletnym, appliancem sprzętowym pochodzącym od  jednego producenta. |
| 53. | Oferowane urządzenie jest objęte min. 3-letnim wsparciem producenta działającym w trybie zgłaszania awarii: 24x7 oraz reakcją NBD. Urządzenie oferowane jest wraz z usługą pozostawienia kupującemu uszkodzonych nośników dyskowych bez konieczności ponoszenia dodatkowych kosztów. |

1. **Biblioteka taśmowa – min. wymagania:**

|  |  |  |
| --- | --- | --- |
| **Lp.** | **Element konfiguracji** | **Parametry techniczne** |
| 1. | Wykorzystana technologia | LTO Ultrium wspierająca technologię partycjonowania nośników. |
| 2. | Obudowa | Typu rack 19”. Wysokość min. 2U - wszystkie elementy do montażu są dostarczone wraz z urządzeniem.  Urządzenie ma zapewniać możliwość instalowania w tej samej obudowie i w tym samym czasie różnych generacji napędów LTO (od LTO-6 wzwyż). |
| 3. | Wbudowane  napędy | Jeden napęd LTO-8 wyposażony w złącze SAS SFF8088. Urządzenie ma mieć możliwość instalowania w tej samej obudowie i w tym samym czasie także napędów LTO z interfejsem FC oraz wspierać technologię LTFS (Linear Tape File System) umożliwiającą kopiowanie danych na taśmę bez konieczności użycia oprogramowania do backupu kompatybilną z systemami Linux, MAC OS i Microsoft. Prędkość zapisu pojedynczego napędu bez kompresji – min. 300 MB/sek. Zainstalowany napęd ma możliwość dynamicznego i płynnego dopasowania prędkości do napływających danych (speed matching) w przedziale od 100 do 300 MB/sek. oferuje funkcję SkipSync zapewniającą dużą szybkość zapisu małych plików bez konieczności zatrzymywania i przewijania kasety oraz stosuje szyfrowanie danych metodą AES 256-bit zgodną ze standardem FIPS 140-2 |
| 4. | Ilość slotów i magazynki | Min. 24 kieszenie na taśmy (urządzenie zostaje dostarczone z kompletem magazynków). Jeżeli licencjonowana jest liczba slotów - wymagane aktywowanie wszystkich slotów i magazynków zainstalowanych w urządzeniu. Wymagana ilość mail slot (I/E): min. 1. Wymiana taśm przez  MailSlot odbywa się bez konieczności wysuwania całego magazynka. |
| 5. | Pojemność | Pojemność bez kompresji – min. 288TB przy obsadzeniu wszystkich slotów na taśmy wyłącznie nośnikami LTO-8 |
| 6. | Zarządzanie | Za pomocą panelu kontrolnego znajdującego się na froncie urządzenia oraz zdalne przez sieć poprzez przeglądarkę internetową (web GUI) za pomocą interfejsu FastEthernet. Musi zapewnioniać wsparcie SNTP, protokołów SSL/TLS i IPv6 oraz możliwość definiowania 4 poziomów zarządzania urządzeniem i dostępem do niego. Urządzenie ma mieć możliwość zabezpieczania swojej konfiguracji na podłączony, poprzez slot USB, PenDrive. Operacja ta powinna być możliwa zarówno poprzez web GUI jak i poprzez panel kontrolny urządzenia. Dodatkowo istnieje możliwość zdalnego wysuwania magazynków, restartowania biblioteki oraz wyłączania zasilania napędów poprzez webGUI. |
| 7. | Dodatkowe  interfejsy | Biblioteka jest wyposażona w interfejs sieciowy, interfejs USB oraz interfejs ADI |
| 8. | Obsługa urządzenia | Istnieje możliwość wymiany napędów, zasilacza, modułu portów zarządzania u użytkownika bez konieczności demontażu urządzenia z szafy przemysłowej oraz bez konieczności zdejmowania pokrywy głównej. Zapewniona jest możliwość wyjmowania magazynków z urządzenia nawet przy braku zasilania. Zarówno napęd jak i zasilacz oraz moduł portów zarządzania są wyposażone w lampki kontrolne, informujące o stanie technicznym i widoczne na tylnej stronie biblioteki. Urządzenie wspiera funkcjonalność Air Gap |
| 9. | Partycjonowanie | Urządzenie posiada funkcję partycjonowania, czyli możliwość stworzenia min. 2 logicznych bibliotek |
| 10. | Wyposażenie | Urządzenie jest wyposażone w czytnik kodów kreskowych, 1x kabel zasilający oraz 1x kabel komunikacyjny konieczny do podłączenia urządzenia do odpowiedniego kontrolera serwera umożliwiającego komunikację z urządzeniem – długość kabla min. 2m. W przypadku, gdyby serwer nie dysponował odpowiednim kontrolerem, taki kontroler mi zostać dostarczony wraz z urządzeniem – interfejs kontrolera: dual SAS 12Gb. Wraz z urządzeniem zostanie musi zostać dostarczony także zestaw 25-ciu identycznych nośników na dane o pojemności natywnej pojedynczego nośnika min. 12TB oraz jednego nośnika czyszczącego wyposażonych w naklejki z kodem kreskowym. Wszystkie dostarczone nośniki muszą być kompatybilne i dedykowane do współpracy z oferowanym urządzeniem |
| 11. | Dodatkowe wymagania | Urządzenie jest musi być kompatybilne z aplikacją Veeam Backup & Replication – kompatybilność z wymienioną aplikacją musi być pisemnie potwierdzona przez producenta urządzenia. |
| 12. | Gwarancja | Min. 36 miesięcy  Zgłaszania awarii dokonuje się wyłącznie poprzez ogólnopolską linię telefoniczną producenta lub autoryzowany serwis  producenta posiadający certyfikat ISO9001 na usługi serwisowe – kontakt z serwisem zapewniony jest w języku polskim. |

**Cześć 3. Dokumentacja Systemu Zarządzania Bezpieczeństwem Informacji (SZBI)**

**I. Ogólne warunki realizacji zamówienia**

1.Przedmiotem zamówienia jest opracowanie przez Wykonawcę dla Zamawiającego systemu zarządzania bezpieczeństwem informacji, zwanego „SZBI“, przeprowadzenie szkoleń, zwanych „Szkoleniami“ wraz przekazaniem materiałów szkoleniowych oraz świadczenie usług asysty wdrożeniowej, zwanych „Usługami asysty“, zgodnie z Umową, zwane „Przedmiotem Umowy“.

2. Przedmiot Umowy będzie realizowany w czterech etapach:

1) Etap I — spotkanie organizacyjne z Zamawiającym dotyczące zakresu bezpieczeństwa informacji oraz systemów zarządzania dla kierownictwa, pełnomocnika bezpieczeństwa informacji i administratora systemów informatycznych;

2) Etap II - analiza działalności Zamawiającego i sporządzenie Sprawozdania;

3) Etap III - opracowanie SZBI oraz usługa asysty;

4) Etap IV - przeprowadzenie szkolenia kadry kierowniczej i przekazanie materiałów szkoleniowych oraz usługa asysty;

zwanych dalej „Etapami“, które szczegółowo określa niniejszy OPZ.

3. Wykonawca zobowiązuje się wykonać Przedmiot Umowy w terminach określonych   
w Umowie.

**II. ETAP I**

W ramach Etapu I Wykonawca:

1) przeprowadzi spotkanie organizacyjne z Zamawiającym dotyczące zakresu bezpieczeństwa informacji oraz systemów zarządzania dla kierownictwa, pełnomocnika bezpieczeństwa informacji i administratora systemów informatycznych o następującą tematykę:

a) Wprowadzenie

• Pojęcia związane z bezpieczeństwem informacji,

• Zarządzanie Bezpieczeństwem Informacji w organizacji, na podstawie obowiązujących przepisów prawa,

• Źródła wymagań i zaleceń — norma ISO 27001 oraz ISO 27002.

b) Planowanie i wdrożenie systemu zarządzania

• Zasady wdrożenia systemu zarządzania bezpieczeństwem informacji,

• Podział ról, zakresów obowiązków oraz odpowiedzialności za system w organizacji,

• Analiza ryzyka bezpieczeństwa informacji,

• Zarządzanie ryzykiem bezpieczeństwa informacji,

• Zabezpieczenia techniczne i organizacyjne,

• Struktura dokumentacji systemu zarządzania,

c) Utrzymanie systemu zarządzania,

• Przegląd systemu zarządzania,

• Doskonalenie systemu zarządzania.

2) Czas trwania spotkania — minimum 2 godziny, w tym 1 przerwa do 10 - minut. Preferowane godziny szkolenia 9.00 — 14.00,

3) Forma organizacji spotkania — stacjonarna,

**III. ETAP II**

1. W ramach Etapu II wykonawca:

1) przeprowadzi analizę zwaną dalej „Analizą“, której celem jest identyfikacja kontekstu SZBI u Zamawiającego, obejmującą w szczególności:

a) obszary działalności Zamawiającego i realizowanych zadań,

b) strukturę organizacyjną Zamawiającego,

c) specyfikę pracy poszczególnych komórek organizacyjnych Zamawiającego,

d) systemy informatyczne użytkowane przez Zamawiającego,

e) rejestry publiczne pozostające we właściwości Zamawiającego,

f) wstępną identyfikację informacji przetwarzanych u Zamawiającego,

g) wstępną identyfikację ryzyk związanych z utratą poufności, integralności i dostępności

informacji przetwarzanych u Zamawiającego - w ramach której Wykonawca dokona oceny

ryzyk i szans niezbędnych do zaprojektowania SZBI — również poprzez weryfikację

działalności Zamawiającego.

2) sporządzi sprawozdanie, zwane dalej „Sprawozdaniem":

a) podsumowujące przeprowadzoną Analizę w zakresie, o którym mowa w ust.1 pkt 1,

b) obejmujące propozycje rozwiązań i zmian w zakresie bezpiecznego przetwarzania

informacji u Zamawiającego i wprowadzenia SZBI,

c) obejmujące wstępną koncepcję SZBI, dostosowaną do potrzeb Zamawiającego, w tym do

ryzyk właściwych dla Zamawiającego, zidentyfikowanych w wyniku Analizy,

w szczególności wskazującą na główne obszary i rodzaje procedur, które powinny zostać uregulowane w SZBI.

2. W celu przeprowadzenia Analizy Zamawiający udostępni Wykonawcy niezbędne, posiadane dokumenty.

3. Sprawozdanie zostanie przekazane Zamawiającemu w formie elektronicznej (opatrzonej kwalifikowanym podpisem elektronicznym) oraz formie papierowej.

4. Celem opracowania przez Wykonawcę wstępnej koncepcji SZBI, Zamawiający wskazuje poniżej ogólny ramowy zarys SZBI: Określenie struktury dokumentacji SZBI, która powinna mieć układ hierarchiczny, tj. opisywać SZBI na różnych poziomach szczegółowości oraz określać zagadnienia, które muszą zostać obligatoryjnie uregulowane:

1) poziom jednostki (Zamawiający) - nadrzędny dokument „Polityka Bezpieczeństwa

Informacji“ Zamawiającego, który określa wymagania i zasady bezpieczeństwa informacji obowiązujące u Zamawiającego oraz sposób organizacji SZBI - z tym dokumentem powinny być spójne pozostałe dokumenty w SZBI,

2) poziom systemów teleinformatycznych - polityka bezpieczeństwa systemów

teleinformatycznych, na które składają się:

— dokument „Polityka Bezpieczeństwa Systemów Teleinformatycznych“, który opisuje wymagania i zasady bezpieczeństwa dla systemów teleinformatycznych,

— odniesienia co do wymagań dotyczących zakresu dokumentacji poszczególnych

systemów teleinformatycznych - np. dokumenty: polityki bezpieczeństwa poszczególnych systemów teleinformatycznych, które opisują w jaki sposób zasady i wymagania bezpieczeństwa zawarte w „Polityce Bezpieczeństwa Informacji“ i „Polityce Bezpieczeństwa Systemów Teleinformatycznych“ są realizowane w danym systemie teleinformatycznym,

3) poziom procedur, instrukcji i regulaminów - procedury, instrukcje, regulaminy i inne dokumenty SZBI tworzone w celu uszczegółowienia zasad opisanych w ww. politykach, dotyczące w szczególności zagadnień:

— bezpieczeństwo zasobów ludzkich,

— bezpieczeństwo fizyczne,

— bezpieczeństwo cyberprzestrzeni,

— bezpieczeństwo danych osobowych,

— bezpieczeństwo informacji niejawnych,

— obsługa incydentów,

— zarządzanie ryzykiem,

— użytkowanie systemów teleinformatycznych u Zamawiającego,

— użytkowanie urządzeń mobilnych.

5. Ramowy zarys SZBI, o którym mowa w ust. 4, nie ma charakteru bezwzględnie wiążącego i stanowi jedynie propozycję Zamawiającego. W przypadku nieuwzględnienia przez Wykonawcę wstępnej koncepcji SZBI ramowego zarysu lub jego poszczególnych elementów, Wykonawca uzasadni powyższe Zamawiającemu.

**IV. ETAP III**

1. W ramach Etapu III Wykonawca, na podstawie wyników Analizy i zaakceptowanego przez

Zamawiającego Sprawozdania, opracuje SZBI wraz z licencją i opieką na okres ważności projektu, dostosowany do potrzeb Zamawiającego.

2. SZBI, który opracuje Wykonawca, stanowić będzie system zarządzania bezpieczeństwem informacji u Zamawiającego.

3. SZBI powinien być zgodny z przepisami ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz. U.z 2024 r. poz. 307, z późn. zm.), aktami wykonawczymi do ww. ustawy, wymaganiami normy PN-ISO/IEC 27001, w tym obejmować czternaście następujących obszarów mających wpływ na bezpieczeństwo w organizacji Zamawiającego:

1) Polityka Bezpieczeństwa Informacji;

2) Organizacja bezpieczeństwa informacji;

3) Bezpieczeństwo zasobów ludzkich;

4) Zarządzanie aktywami;

5) Kontrola dostępu;

6) Kryptografia;

7) Bezpieczeństwo fizyczne i środowiskowe;

8) Bezpieczna eksploatacja;

9) Bezpieczna komunikacja;

10) Pozyskiwanie, rozwój i utrzymanie systemów;

11) Relacje z dostawcami;

12) Zarządzanie incydentami związanymi z bezpieczeństwem informacji;

13) Aspekty bezpieczeństwa w zarządzaniu ciągłością działania;

14) Zgodność z wymaganiami prawnymi i własnymi standardami.

Ponadto, SZBI powinien uwzględniać wymagania norm: PN-ISO/IEC 27002, PN-ISO/IEC

27005 oraz PN-ISO/IEC 24762.

4. SZBI musi być zgodny z aktualnymi przepisami powszechnie obowiązującego prawa,

w szczególności z przepisami:

1) rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679z dnia 27 kwietnia 2016 r.

w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych

i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne

rozporządzenie o ochronie danych) (Dz. Urz. UE L 119 z 04.05.2016, str. 1);

2) ustawy z dnia 10 maja 2018 r.o ochronie danych osobowych;

3) ustawy z dnia 17 lutego 2005 r.o informatyzacji działalności podmiotów realizujących zadania

publiczne;

4) ustawy z dnia 6 września 2001 r. o dostępie do informacji publicznej;

5) ustawy z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych;

6) ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa;

7) Rozporządzenia Rady Ministrów z dnia 21 maja 2024r. w sprawie Krajowych Ram

Interoperacyjności minimalnych wymagań dla rejestrów publicznych i wymiany informacji

w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych

8) Dyrektywy Parlamentu Europejskiego i Rady (UE) 2022/2555 z dnia 14 grudnia 2022 r.

w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na

terytorium Unii, zmieniająca rozporządzenie (UE) nr 910/2014i dyrektywę (UE) 2018/1972

oraz uchylająca dyrektywę (UE) 2016/1148.

5. W ramach opracowania SZBI Wykonawca między innymi:

1) zaproponuje obszary funkcjonalne, które powinny zostać objęte SZBI, spójne z treścią Sprawozdania zaakceptowanego przez Zamawiającego;

2) uwzględnienie w szczególności następujących zagadnień:

a) określenie organizacji bezpieczeństwa informacji,

b) identyfikacja aktywów informacyjnych i klasyfikacji informacji przetwarzanych   
u Zamawiającego,

c) szacowanie ryzyka oraz postępowania z ryzykiem, związanych z utratą poufności, integralności i dostępności informacji przetwarzanych u Zamawiającego,

d) bezpieczeństwo w procesach zarządzania zasobami ludzkimi,

e) szkolenia z zakresu bezpieczeństwa informacji,

f) kontrola dostępu,

g) bezpieczeństwo fizyczne i środowiskowe,

h) klasyfikacja informacji,

i) odpowiedzialność za zasoby,

j) postępowanie z nośnikami informacji,

k) użytkowanie urządzeń mobilnych i praca zdalna,

I) zarządzanie sprzętem informatycznym,

m) instalacja oprogramowania,

n) ochrona przed oprogramowaniem złośliwym,

o) kopie zapasowe,

p) zarządzanie zmianami, w szczególności w systemach informatycznych oraz

infrastrukturze informatycznej,

q) zarządzanie dokumentacją infrastruktury informatycznej,

r) monitorowanie systemów informatycznych,

s) zarządzanie pojemnością systemów,

t) serwis i konserwacja infrastruktury informatycznej,

u) zarządzanie podatnościami technicznymi,

v) zarządzanie incydentami bezpieczeństwa,

w) zabezpieczenia kryptograficzne,

x) bezpieczeństwo sieci i transmisji danych,

y) ochrona własności intelektualnej,

z) bezpieczeństwo informacji w relacjach z dostawcami,

aa) ciągłość działania,

bb) zasady bezpieczeństwa informacji w procesach pozyskiwania, rozwoju i utrzymania

systemów informacyjnych,

cc) weryfikacja zgodności z wymaganiami prawnymi,

dd) korzystanie z poczty elektronicznej i Internetu,

ee) zarządzanie usługami informatycznymi,

ff) utrzymanie i doskonalenie SZBI,

gg) przeprowadzanie audytów SZBI.

6. Wykonawca wraz z SZBI przedstawi zestawienie, zwane „Zestawieniem, w którym wykaże spełnienie przez SZBI wymagań dotyczących bezpieczeństwa informacji wynikających z aktualnych przepisów powszechnie obowiązującego prawa, a także odpowiednich norm.

7. SZBI oraz Zestawienie zostaną przekazane Zamawiającemu w formie elektronicznej (opatrzonej kwalifikowanym podpisem elektronicznym) oraz w formie papierowej.

**V. ETAP IV**

1. W ramach Etapu IV Wykonawca:

1) przeprowadzi szkolenie (trwające min. 4h) dla osób odpowiedzialnych u Zamawiającego za funkcjonowanie SZBI (maksymalnie 4 osób) obejmujące w szczególności:

a) omówienie podstawowych zasad bezpieczeństwa informacji i wypełniania procedur, wynikających z SZBI,

b) zagrożenia związane z przetwarzaniem informacji u Zamawiającego,

c) zapoznanie z nowym SZBI, w szczególności poprzez przedstawienie Zamawiającemu głównych obszarów, poszczególnych ścieżek procedur i zasad reagowania na incydenty, wynikających z SZBI,

d) odpowiedzialność za naruszenie zasad związanych z SZBI;

2) przygotuje materiały szkoleniowe w formie pliku elektronicznego, wskazujące na istotę funkcjonowania SZBI, uwzględniające główne obszary SZBI i wynikające z nich procedury, zaprezentowane w sposób syntetyczny i przejrzysty (np. ilustracje, schematy, tabele), dostosowane do potrzeb Zamawiającego. Materiały te zostaną udostępnione pracownikom Zamawiającego (np. w ramach wewnętrznej sieci Intranet) celem zapoznania ich z problematyką związaną z bezpieczeństwem informacji, a także nową dokumentacją w tym zakresie. Materiały te mają stanowić uniwersalne i praktyczne kompendium wiedzy, omawiające najistotniejsze zagadnienia związane z bezpieczeństwem informacji u Zamawiającego.

2. Szczegółowe programy szkolenia i ich dokładne terminy, a także materiały szkoleniowe zostaną zaproponowane przez Wykonawcę i będą wymagały akceptacji Zamawiającego.

3. Szkolenie zostanie przeprowadzone w siedzibie Zamawiającego (szkolenie stacjonarne).

Dodatkowo zamawiający wymaga by dokumentacja SZBI, była aktualizowana i dostosowywana do zmieniających się przepisów oraz powiązanych innych dokumentów z SZBI przez min. 3 lata od podpisania umowy.

Wymagane też prowadzenie dokumentacji w sposób elektroniczny w częściach podlegających ciągłej zmianie i gdzie jest to możliwe.