**SZCZEGÓŁOWY OPIS PRZEDMIOTU ZAMÓWIENIA**

**Wdrożenie systemu DLP**

**SPIS TREŚCI**

[1 SŁOWNIKI I SKRÓTY 3](#_Toc513470924)

[2 PRZEDMIOT ZAMÓWIENIA 3](#_Toc513470925)

[3 WYMAGANIA 5](#_Toc513470926)

[3.1 Opracowanie koncepcji wdrożenia 5](#_Toc513470927)

[3.2 System DLP 5](#_Toc513470928)

[3.3 Wymagania dot. wdrożenia systemu DLP 13](#_Toc513470929)

[3.4 Wymagania dotyczące szkoleń użytkowników 15](#_Toc513470930)

[3.5 Materiały szkoleniowe 15](#_Toc513470931)

[3.6 Dokumentacja 16](#_Toc513470932)

[4 WYMAGANIA W ZAKRESIE OZNAKOWANIA DOKUMENTACJI 18](#_Toc513470933)

[5 GWARANCJE, WYMAGANIA PRAWNE i INNE WYMAGANE PARAMETRY TECHNICZO-UŻYTKOWE 19](#_Toc513470934)

# SŁOWNIKI I SKRÓTY

Dla potrzeb niniejszego opracowania przyjmuję się następujące definicje skrótów i pojęć:

| **Skrót/pojęcie** | **Definicja** |
| --- | --- |
| **DLP** | (Data Loss Prevention) - Oprogramowanie zapewniające ochronę danych w postaci elektronicznej przed kradzieżą lub przypadkowymi wyciekami. |
| **Incydent** | Związany z bezpieczeństwem informacji, rozumiany jako pojedyncze zdarzenie lub seria niepożądanych zdarzeń związanych z bezpieczeństwem, które stwarzają znaczne prawdopodobieństwo zakłócenia działań biznesowych i zagrażają bezpieczeństwu informacji. |

Pozostałe pojęcia użyte w dokumencie należy rozumieć zgodnie z ich ogólnie przyjętym znaczeniem.

# PRZEDMIOT ZAMÓWIENIA

Przedmiotem zamówienia jest:

* Dostarczenie systemu ochrony informacji przed wyciekiem (system DLP) w ramach licencji,
* Wdrożenie i zintegrowanie dostarczonego systemu DLP,
* Zapewnienie wsparcia na etapie dostrajania systemów
* Zapewnienie wsparcia w zakresie dostarczonych licencji na system DLP oraz wsparcie Wykonawcy w zakresie usuwania problemów przy bieżącej eksploatacji systemu przez okres 24 miesięcy,

Przedmiot zamówienia obejmuje następujące etapy:

|  |  |  |  |
| --- | --- | --- | --- |
| **Etapy** | **Przedmiot zamówienia** | **Maksymalny czas wyznaczony do realizacji Etapu** | **Minimalny czas wymagany do realizacji poszczególnych zadań w ramach Etapu** |
| **Etap 1** | 1. Opracowanie koncepcji wdrożenia na podstawie analiz, wywiadów Wykonawcy i dokumentacji przekazanej przez Zamawiającego.
2. Przekazanie dokumentacji koncepcji wdrożenia.
 | **10 dni roboczych** **od dnia podpisania Umowy** | 3 dni robocze na czynności odbiorcze Zamawiającego |
| **Etap 2** | 1. Dostawa, instalacja i wdrożenie Systemu DLP wraz z regułami.
2. Dostarczenie dokumentacji szkoleniowej (materiałów szkoleniowych) dla użytkowników DLP.
3. Przeprowadzenie szkoleń.
4. Dostarczenie dokumentacji powdrożeniowej.
 | **20 dni roboczych od daty zakończenia Etapu 1 potwierdzonego protokołem odbioru** | 5 dni roboczych na czynności odbiorcze Zamawiającego |
| **Etap 3** | 1. Dostrajanie reguł, systemu DLP i systemów Zamawiającego.
2. Aktualizacja dokumentacji.
 | **90 dni roboczych od daty zakończenia etapu 2** | 5 dni roboczych na czynności odbiorcze Zamawiającego |
| **Gwarancja** | 1. Objęcie gwarancją wdrożonego systemu DLP i świadczenie usługi wsparcia zdalnego w Etapie 2 i 3
 | **24 miesięcy od daty zakończenia Etapu 2 potwierdzonego protokołem odbioru** | 5 dni roboczych na czynności odbiorcze Zamawiającego |

# WYMAGANIA

Przedmiotem zamówienia jest dostawa i wdrożenie systemu ochrony przed wyciekami informacji, będący rozwiązaniem programowym (nie urządzeniem typu appliance), który zostanie zainstalowany w infrastrukturze Zamawiającego, opracowanie dokumentacji i przeprowadzenie szkoleń dla użytkowników CPPC.

O ile inaczej nie zaznaczono, wszelkie zapisy zawierające parametry techniczne należy odczytywać jako parametry minimalne.

## Opracowanie koncepcji wdrożenia (analizy przedwdrożeniowej)

Wykonawca opracuje koncepcję wdrożenia systemu DLP w Centrum Projektów Polska Cyfrowa. Koncepcja zostanie opracowana na podstawie materiałów dostarczonych po podpisaniu umowy, w postaci klasyfikacji informacji i zasady postępowania z informacjami opracowanej zgodnie z normą ISO 27001 oraz na podstawie informacji pozyskanych z przeprowadzonych wywiadów i analiz u Zamawiającego.

Koncepcja powinna zawierać:

* Harmonogram realizacji Etapu 2. Harmonogram musi uwzględniać terminy wdrożeń, testów i odbiorów. Harmonogram, będzie podstawą do realizacji umowy;
* Projekt wdrożenia systemu w systemach Zamawiającego;
* Projekt reguł i polityk zabezpieczeń w ramach systemu DLP;
* Plan testów akceptacyjnych wdrożonych zabezpieczeń, takich jak: scenariusze testowe reguł i polityk, testy wydajności, testy bezpieczeństwa dot. odporności systemu w kontekście zapewnienia poufności, integralności i dostępności, testy wymagań funkcjonalnych i niefunkcjonalnych;
* Wykonawca przekaże Zamawiającemu jeden egzemplarz podpisanej Koncepcji Wdrożenia oraz wersję elektroniczną w niezabezpieczonym/edytowalnym formacie MS Word i niezabezpieczonym formacie PDF (na płycie CD/DVD lub innym równoważnym nośniku danych).

## System DLP

System DLP powinien składać się z serwera zarządzającego wyposażonego w konsolę zarządzającą oraz końcówki – oprogramowanie agentowe, które będzie instalowane na stacjach roboczych. System musi spełniać co najmniej następujące wymagania:

|  |  |
| --- | --- |
| **Kod wymagania** | **Opis wymagania** |
| DLP.01 | System DLP wraz z komponentami musi być dostarczony z bezterminową licencją uprawniającą do użytkowania oprogramowania. |
| DLP.02 | System DLP musi umożliwiać wykrywanie i ochronę przed wyciekiem informacji przesyłanej przez sieć (poza strukturę Zamawiającego) oraz w ramach urządzeń stacji roboczych i serwerach Zamawiającego. |
| DLP.03 | System DLP musi mieć możliwość identyfikacji, klasyfikacji i lokalizacji chronionych dokumentów, informacji znajdujących się w zasobach Zamawiającego a w szczególności na stacjach roboczych (komputery PC i urządzenia mobilne z systemem Android i iOS), serwerach, systemie poczty elektronicznej. |
| DLP.04 | Wymagane jest by komunikacja z użytkownikiem (przesyłanie przez system DLP informacje do użytkownika o naruszeniu zasad polityki bezpieczeństwa) odbywała się w języku polskim i było możliwe jego dowolne dostosowanie. |
| DLP.05 | Zamawiający dopuszcza język angielski w konsoli administratora oraz audytu. |
| DLP.06 | Zamawiający oczekuje dostarczenia licencji dla następującej liczby użytkowników:* + - 1. ochrona i wykrywanie danych na poziomie stacji roboczej (komputery PC z systemem Windows 7 i nowszym): 180 komputerów,
			2. ochrona i wykrywanie danych na poziomie urządzenia mobilnego (system Android, iOS): 90 urządzeń mobilnych,
			3. ochrona sieciowa przesyłanych danych: 180 użytkowników
			4. wykrywanie danych na zasobach wspólnych: 180 użytkowników (dane na serwerach plików)
			5. Szyfrowanie udostępnianych plików: 30 użytkowników

Zamawiający dopuszcza dostarczenie innych licencji w ramach proponowanego rozwiązania, które pozwolą na realizację minimalnych wymagań w ramach tego OPZ. |
| DLP.07 | Wykonawca musi zapewnić wsparcie producenta w zakresie dostarczonych licencji oraz w zakresie usuwania problemów przy bieżącej eksploatacji systemu przez okres 24 miesięcy. Zamawiający oczekuje, że wsparcie będzie realizowane w języku polskim. |
| DLP.08 | System musi realizować swoje funkcje na poziomie sieci i infrastruktury Zamawiającego oraz na poziomie stacji roboczych. Realizacja funkcji ochrony informacji na poziomie sieci i na poziomie stacji roboczych powinna być rozłączna co oznacza, że Zamawiający zastrzega sobie prawo do wskazania w grupie komputerów chronionych na poziomie sieciowym komputerów, które maja być objęte dodatkową ochroną na poziomie stacji roboczej. |
| DLP.09 | System musi realizować ochronę przed wyciekiem informacji z systemów informatycznych Zamawiającego poprzez blokowanie lub/i monitowanie akcji w momencie wykrycia niedozwolonej interakcji użytkownika. |
| DLP.10 | System musi umożliwiać identyfikację miejsc przetwarzania i przechowywania informacji chronionych (np. stacje robocze PC z systemem Windows, urządzenia mobilne, serwery plików, serwer poczty Microsoft Exchange, Chmura Nextcloud). |
| DLP.11 | Instalacja agenta systemu DLP nie może wymagać ponownego uruchomienia systemu (restart). |
| DLP.12 | Ochrona informacji powinna odbywać się w oparciu o reguły bezpieczeństwa informacji odzwierciedlające zdefiniowane przez Zamawiającego na etapie wdrożenia. |
| DLP.13 | System musi umożliwiać monitorowanie i ochronę wielu kanałów komunikacyjnych, w szczególności:* + - 1. Wsparcie dla protokołów HTTPS, HTTP, FTP, Secure FTP
			2. e-mail (w tym załączniki), protokoły IMAP, POP3, SMTP, Exchange,
			3. komunikatory internetowe
			4. Wsparcie dla przeglądarek Chrome, Firefox, Internet Explorer i Edge
 |
| DLP.14 | System musi wykonywać inspekcję ruchu szyfrowanego SSL. |
| DLP.15 | System musi wspierać inspekcję systemów Outlook/Exchange, File Server, MS Excel, MS Word, MS PowerPoint. |
| DLP.16 | Agent system DLP musi umożliwiać wykrywanie i blokowanie informacji chronionych znajdujących się w plikach zapisywanych przez aplikacje z pakietu Microsoft Office (w tym w plikach Word XML Document, XPS Document, Word Macro - Enabled Document) |
| DLP.17 | Agent musi umożliwiać wykrywanie i blokowanie informacji chronionych znajdujących się w plikach zapisywanych przez aplikacje LibreOffice oraz Open Office. |
| DLP.18 | Agent systemu DLP nie może modyfikować dokumentów, metadanych opisujących właściwości dokumentów ani dodawać lub modyfikować atrybutów systemu plików (z wyłączeniem czasu dostępu do pliku – Last Access Time). |
| DLP.19 | Agent musi umożliwiać blokowanie użycia funkcji „zrzut ekranu” (ang. printscreen). |
| DLP.20 | System musi umożliwiać definiowanie własnych kanałów transmisji, które mają być monitorowane a w szczególności musi wykrywać poufną informację w ramach protokołów funkcjonujących o dowolnie ustawiane porty. |
| DLP.21 | System musi umożliwiać tworzenie polityk uwzględniających takie akcje jak:* + - 1. wysyłanie powiadomień w ramach odnotowanych incydentów, przy czym system powinien mieć możliwość zdefiniowania osób, którym taka informacja ma być przesłana (np. nadawca, zwierzchnik nadawcy, właściciel informacji (polityki), audytor bezpieczeństwa informacji)
			2. blokowanie transmisji naruszających zdefiniowaną politykę,
			3. kwarantannę informacji,
			4. okno dialogowe z predefiniowanym tekstem w ramach polityki, wymuszające dodatkową interakcję użytkownika, np. możliwość określania przez użytkownika powodu wykonania czynności przez użytkownika, która została zidentyfikowana jako incydent.
			5. szyfrowanie informacji w sposób umożliwiający kontrolę nad dostępem do zawartości nawet po przesłaniu zaszyfrowanego pliku poza organizację (każdorazowe otwarcie zaszyfrowanego pliku wymaga połączenia z serwerem Zamawiającego i sprawdzenia czy uprawnienia do odczytu nie zostały wycofane),
			6. zrzut ekranu z wykonywanej przez użytkownika czynności.
 |
| DLP.22 | System musi umożliwiać łączenie polityk w grupy. |
| DLP.23 | System musi umożliwiać budowanie polityk ochrony informacji uwzględniając kontekst w jakim informacja jest używana, czyli musi uwzględniać okoliczności takie jak:* + - 1. co jest wysyłane (jaka kategoria danych),
			2. kto wysyła informacje,
			3. gdzie (do kogo) są wysyłane informacje,
			4. jakim kanałem są wysyłane informacje (e-mail, zaszyfrowany e-mail, strona www, protokoły transmisji plików itp.)
			5. System musi umożliwiać budowanie polityk chroniących przed wyciekiem danych w kanale HTTP oraz HTTPS bazujących na kategorii, np. blokować wypływ danych do stron z kategorii „Botnet” oraz „Compromised websites”.
 |
| DLP.24 | System musi wykorzystywać informacje zawarte w metadanych dokumentów oraz dane wprowadzone do dokumentów przez narzędzia do klasyfikacji i etykietowania (tagowania) dokumentów i wiadomości e-mail. |
| DLP.25 | System musi wykorzystywać szeroką gamę mechanizmów identyfikowania treści, m.in.:* + - 1. słowa kluczowe,
			2. wyrażenia regularne,
			3. tzw. odcisk palca (fingerprint),
			4. algorytmy Machine Learning.
 |
| DLP.26 | Algorytm tworzenia odcisku palca powinien tworzyć wiele odcisków palca dla pojedynczego pliku, tak aby chronić informacje zawarte w pliku a nie wyłącznie dokument w całości. |
| DLP.27 | System powinien również umożliwić tworzenie odcisków palca z zasobów zawartych w bazach danych. Tworzenie takich odcisków powinno odbywać się bez uprzedniego kopiowania informacji do pliku (np. za pomocą ODBC). |
| DLP.28 | System musi zawierać predefiniowane reguły ochrony informacji, dotyczących danych osobowych (np. PESEL, REGON, NIP, nr Dowodu Osobistego) oraz bankowych (np. numerów kart kredytowych, IBAN). Przede wszystkim system musi wspierać ochronę danych prawnie chronionych oraz informacji stanowiących tajemnice przedsiębiorstwa. |
| DLP.29 | System powinien umożliwiać rozpoznawanie tekstu zawartego w plikach graficznych i jego analizę pod względem wrażliwości informacji (OCR). Moduł OCR wchodzi w skład oprogramowania które dostarczy Wykonawca. |
| DLP.30 | System musi umożliwiać zautomatyzowane wykrywanie informacji objętych politykami ochrony na serwerach i stacjach końcowych w sieci Zamawiającego. Funkcjonalność ta powinna być również oferowana dla folderów Exchange, plików PST. |
| DLP.31 | System musi umożliwiać nabycie przez Zamawiającego szczegółowej wiedzy o osobach z dostępem do informacji chronionych oraz zakresie przesyłania tych informacji |
| DLP.32 | W ramach ochrony informacji na stacji roboczej system musi umożliwiać monitorowanie/blokowanie takich czynności jak kopiowanie informacji na zewnętrzne nośniki danych, kopiowanie do schowka systemowego, nagrywanie płyt CD/DVD, USB, FireWire, pamięci Flash/CompactFlash, drukowanie (również lokalne), wklejanie informacji w okna aplikacji webowych, wysyłanie informacji za pomocą poczty elektronicznej (MS Outlook, MS OWA dla Exchange) itp. Zamawiający posiada stacje robocze z systemem operacyjnym Windows 7, Windows 10. |
| DLP.33 | Agent systemu DLP musi umożliwiać wykrywanie i blokowanie podczas kopiowania chronionej informacji za pomocą dowolnej aplikacji do zarządzania plikami (np. Windows Explorer, Norton/Total/Free Commander) oraz interpretera poleceń cmd.exe. |
| DLP.34 | System musi wspierać możliwość inspekcji spakowanych plików, w zakresie co najmniej następujących formatów danych np: ZIP, RAR. |
| DLP.35 | Agent systemu DLP musi wymuszać politykę ochrony informacji również w przypadku, gdy stacja robocza nie jest podłączona do sieci (tzw. tryb pracy offline). |
| DLP.36 | Agent systemu DLP musi posiadać możliwość rozpoznawania typów plików po nagłówku pliku lub rozszerzeniu w celu stworzenia polityk dotyczących kopiowania, wysłania i audytowania plików. |
| DLP.37 | System musi posiadać możliwość blokowania plików archiwum, które są zabezpieczone hasłem jeśli nie ma możliwości ich inspekcji. |
| DLP.38 | Wszystkie funkcje zarządzania systemem DLP (ochrona informacji w sieci, wykrywanie chronionych informacji i ochrona informacji na poziomie stacji roboczej) powinny być osiągalne z jednej konsoli zarządzającej. |
| DLP.39 | Dostęp do konsoli zarządzającej powinien odbywać się przez przeglądarkę internetową, przez protokół HTTPS. |
| DLP.40 | Konsola zarządzająca powinna umożliwiać zarządzanie incydentami, m.in. zmianę ich statusu, przekazywanie do innego administratora. |
| DLP.41 | System musi umożliwić ziarnistą delegację uprawnień do konfiguracji systemu, polityk, raportów oraz incydentów w oparciu o wbudowane jak również własne role, takie jak administrator, audytor, manager incydentów. |
| DLP.42 | System w ramach odnotowanych incydentów musi udostępniać informacje dotyczące reguły, która została naruszona, jak również kopię – lub fragment informacji, która była przesyłana, wraz z informacją jakie działanie zostało wykonane w ramach zdefiniowanej polityki. |
| DLP.43 | System DLP musi umożliwiać rejestrowanie informacji i danych historycznych o zgromadzonych incydentach w celu ich późniejszej analizy. |
| DLP.44 | System DLP musi posiadać moduł wyszukiwania kontekstowego w logach audytu i alertów (nadawca, odbiorca, usługa, rodzaj naruszenia polityki, źródło naruszenia) oraz musi posiadać następujące funkcjonalności:1. możliwość zaimplementowania usługi automatycznego indeksowania zgromadzonych centralnie logów audytu i plików shadowingu w celu szybkiego kontekstowego wyszukiwania określonych przez administratora treści
2. możliwość określenia nadawcy i odbiorcy (usługi poczty, komunikatory) oraz typu plików i źródła.
 |
| DLP.45 | System DLP musi wspierać komunikację S/MIME wykorzystywaną przez oprogramowanie MS Exchange / Outlook Zamawiającego oraz infrastrukturę PKI. |
| DLP.46 | System DLP musi umożliwiać kontrolowanie dostępu na poziomie użytkownika lub grupy użytkowników do:1. portów USB i Fire Wire, IrDA, COM, LPT
2. urządzeń WiFi oraz Bluetooth (także wbudowanych)
3. dowolnego typu drukarek, włącznie z drukarkami lokalnymi, sieciowymi i wirtualnymi
4. urządzeń PDA i smartfonów wykorzystujących system Android, Windows Mobile i Apple iOS
5. urządzeń zewnętrznych podłączanych do komputera umożliwiających zapis/odczyt chronionych danych
6. urządzeń pracujących pod kontrolą protokołu MTP
7. napędów optycznych CD/DVD/BR i napędów taśmowych
8. schowka systemowego (z możliwością określenia typu kopiowanych danych: tekst, pliki graficzne, pliki audio, zrzuty ekranu)
9. mapowanych dysków dla sesji terminalowych
10. urządzeń USB, portów COM dla sesji terminalowych
11. schowka systemowego na poziomie sesji terminalowych
12. dysków HDD
13. możliwość kontroli dostępu do urządzeń zewnętrznych podłączanych do komputerów w określonych dniach tygodnia i godzinach
14. granularna kontrola danych synchronizowanych z urządzeniami/smartfonami z systemem Android, Windows Mobile, iOS (synchronizacja kalendarza, poczty, plików, kontaktów itp.)
15. tworzenie „białej listy urządzeń USB, która pozwoli na autoryzację tylko wybranych urządzeń (model lub unikatowy numer urządzenia)
16. możliwość przypisania urządzeń USB z białej listy do określonych użytkowników lub grupy użytkowników
17. zdalne dopisywanie urządzeń USB do bazy danych urządzeń
18. możliwość włączenia audytu i shadowingu (tworzenia cienia danych) dla urządzeń USB dodanych do białej lisy
19. tworzenie „białej listy nośników CD/DVD, która umożliwia autoryzację tylko wybranych nośników
20. możliwość określenia rodzajów urządzeń, które mają być kontrolowane (urządzenia typu HID, drukarka, skaner, itp.)
21. zdalne odblokowywanie urządzeń USB (tymczasowa biała lista) za pomocą specjalnie wygenerowanego kodu
22. możliwość ustalania różnych polityk dostępu do urządzeń dla trybu pracy online (praca w firmie) i pracy offline (praca poza firmą) przy zachowaniu tego samego konta użytkownika
23. integracja z oprogramowaniem do szyfrowania pozwalająca ograniczyć kopiowanie danych do urządzeń szyfrowanych oprogramowaniem: Windows Bit Locker To Go, VeraCrypt, macOS FileVault, Drive Crypt, PGP Whole Disk Enchirydion, SafeToGo, SafeDisk lub sprzętowych szyfrowanych nośników wymiany danych
24. wykrywanie sprzętowych keyloggerów (PS/2 oraz USB)
25. wsparcie dla sesji terminalowych (Microsoft RDS, Citrix XenDesktop/XenApp, Citrix XenServer, VMware Horizon View; VMware Workstation, VMware Player, Oracle VM VirtualBox)
26. rozpoznawanie typów kopiowanych plików po nagłówkach z możliwością przypisania określonych przez administratora reguł bezpieczeństwa
 |
| DLP.47 | System DLP powinien posiadać następujące funkcjonalności w obszarach monitorowania ruchu sieciowego:1. kontroli ruchu sieciowego na poziomie użytkownika lub grupy użytkowników
2. kontrola ruchu sieciowego oraz aplikacji i usług sieciowych
3. kontrola wybranych usług sieciowych web mail: MAPI (Microsoft Exchange), SMTP/SMTPS, IBM Notes (Lotus Notes), Gmail, Yahoo! Mail, Hotmail (Outlook.com), AOL Mail, Microsoft Outlook Web App (OWA, formerly Outlook Web Access), Rambler Mail, Yandex Mail
4. kontrola ruchu do sieci społecznościowych (Facebook (+API), Twitter, Google+, LinkedIn, Tumblr, MySpace, Vkontakte (+API), XING.com, LiveJournal, Disqus)
5. kontrola udostępnianianych plików w chmurze (Dropbox, SkyDrive, Google Drive, Amazon S3, Microsoft OneDrive, Google Drive, Box, OneDrive/SkyDrive, iCloud, Amazon S3, Yandex Disk
6. kontrola komunikatorów sieciowych (Skype, ICQ/AOL, Windows Live Messenger, Yahoo! Messenger, IRC, Jabber, WhatsApp Web)
7. kontrola ruchu sieciowego (reguły) w określonych dniach tygodnia i godzinach
8. kontrola danych wysyłanych przez formularze POST
9. kontrola wysyłanych plików (załączniki pocztowe, komunikatory, sieci społecznościowe)
10. możliwość tworzenia tzw. „białej listy protokołów (typ protokołu, port), stron internetowych (domena, adres IP) , usług sieciowych
11. możliwość ustawienia kontroli dostępu obejmującej następujące protokoły sieciowe: FTP/FTPS, HTTP/HTTPS, SMB, SMTP, MAPI, Telnet w określonych dniach tygodnia i godzinach
12. wbudowany firewall pozwalający na blokadę określonego ruchu sieciowego (protokół, port, domena, IP)
13. możliwość ustalania różnych polityk dla trybu pracy online (praca w firmie) i pracy offline (praca poza firmą) przy zachowaniu tego samego konta użytkownika
14. blokowanie ruchu PROXY
15. blokowanie wychodzącego niezidentyfikowanego ruchu SSL
 |
| DLP.48 | System DLP musi posiadać funkcje audytu i shadowing danych przesyłanych przez sieć oraz obejmować następujące obszary:1. audytowanie oraz alertowanie w czasie rzeczywistym o zdarzeniach związanych z transferem danych przez sieć
2. nawiązanie połączenia, odbierane i wysłanie plików, formularze POST, wychodzące i przychodzące wiadomości
3. tworzenie cienia przesyłanych przez sieć danych (shadowing) dla aplikacji i usług sieciowych korzystających z następujących protokołów: FTP/FTPS, HTTP/HTTPS, SMB, SMTP, MAPI.
4. odbierane i wysłanie plików, formularze POST, wychodzące i przychodzące wiadomości,
5. gromadzenie centralnie lub lokalnie logów audytu oraz plików shadowing
6. wysyłanie powiadomień z wykorzystaniem poczty elektronicznej lub integracja z systemem powiadamiania o zdarzeniach opartym o protokół SNMP lub SYSLOG
 |
| DLP.49 | System DLP musi oferować integracje z bazą LDAP w następujących obszarach:1. zarządzanie z poziomu GPO serwera domenowego (integracja z AD)
2. wsparcie dla RSoP (przystawka wynikowy zestaw zasad)
3. zarządzanie z poziomu konsoli web
4. możliwość definiowania kont administracyjnych z przydziałem odpowiednich ról
5. zdalna instalacja agenta bez konieczności ponownego uruchamiania komputera
6. ochrona agenta przed nieautoryzowanym zatrzymaniem
7. możliwość zaimplementowania usługi centralnego gromadzenia logów audytu i plików shadowingu
 |
| DLP.50 | System DLP musi posiadać możliwość tworzenia spersonalizowanych:1. raportów z logów audytu i plików shadowingu w formacie pdf, html lub doc (np: najbardziej aktywni użytkownicy, liczba przekopiowanych plików, liczba wydrukowanych dokumentów)
2. raportu relacji między użytkownikami obrazującego połączenia dla następujących protokołów i usług: ICQ / AOL Messenger, IRC, Jabber, Skype, Yahoo Messenger, MAPI, IBM Notes, SMTP, Web Mail oraz sieci społecznościowe.
3. raportów wysłanych za pośrednictwem poczty elektronicznej
4. możliwość filtrowania dzienników aktywności w oparciu o określone typy informacji (np. nazwa użytkownika, nazwa komputera, źródło informacji, proces, data/czas zdarzenia, rodzaj akcji)
5. możliwość monitorowania w czasie rzeczywistym stanu zainstalowanych na stacjach roboczych agentów
 |

## Wymagania dot. wdrożenia systemu DLP

|  |  |
| --- | --- |
| **Kod wymagania** | **Opis wymagania** |
| WDLP.01 |  Oprogramowanie systemu DLP należy zainstalować na infrastrukturze wskazanej przez Zamawiającego. |
| WDLP.02 | Zainstalowany system musi być skonfigurowany i uruchomiony do pracy. |
| WDLP.03 | System DLP musi umożliwiać klasyfikację informacji przy pomocy oznaczania (tagowania) dokumentów i informacji przez użytkownika lub/i automatycznie na podstawie reguł. Klasyfikacja informacji powinna być zintegrowana co najmniej z oprogramowaniem MS Office i MS Outlook używanym przez Zamawiającego. |
| WDLP.04 | System musi współpracować z systemem Symantec Messaging Gateway używanym aktualnie przez Zamawiającego. |
| WDLP.05 | System w ramach dostarczonych licencji musi być wdrożony w środowisku wirtualnym Zamawiającego. Zamawiający dysponuje systemami operacyjnymi: Microsoft Windows Server 2012 R2 oraz Linux pracującymi w środowisku wirtualnym VMWare 6.x. |
| WDLP.06 | Dostarczenie licencji i instalacja oprogramowania systemu. Instalację oprogramowania na stacjach roboczych wykonają pracownicy Zamawiającego w ramach GPO na podstawie informacji i dokumentacji dostarczonej przez Wykonawcę. |
| WDLP.07 | W ramach prac wdrożeniowych, Wykonawca przeprowadzi analizę przedwdrożeniową polegającą na weryfikacji możliwości wdrożenia systemu DLP na podstawie opracowanego przez Zamawiającego wykazu klasyfikacyjnego informacji chronionej. Wykonawca zrealizuje adaptację ww. wykazu klasyfikacyjnego informacji chronionej do wymagań elektronicznej ochrony informacji systemem DLP i ich wdrożenie w zakresie 5 (pięciu) wskazanych przez Zamawiającego polityk bezpieczeństwa (obszarów chronionych danych) DLP (polityki te nie mogą się pokrywać z predefiniowanymi w oferowanym przez Wykonawcę systemie politykami – o ile oferowany system taki predefiniowany zestaw posiada). |
| WDLP.08 | Ustalenie kryteriów progowych dla wykrywanych zdarzeń dla poszczególnych obszarów chronionych danych. |
| WDLP.09 | Wypracowanie szczegółowego modelu pozyskiwania wzorcowych danych dla systemu. |
| WDLP.10 | Instalacja i wstępna konfiguracja systemu, w tym zdefiniowanie reguł dotyczących identyfikacji danych osobowych oraz polityk ochrony danych osobowych zgodnych z GDPR (RODO). |
| WDLP.11 | Opracowanie wytycznych oraz przygotowanie kontenerów instalacyjnych dla oprogramowania Agentów DLP. |
| WDLP.12 | Opracowanie i wykonanie konfiguracji ustawień Agentów DLP. |
| WDLP.13 | Instalacja i konfiguracja systemu OCR dokumentów przesyłanych w sieci (system OCR należy dostarczyć w ramach zadania). |
| WDLP.14 | Konfiguracja systemu i uruchomienie produkcyjne zgodnie z przyjętymi i uzgodnionymi z Zamawiającym procesami i procedurami biznesowymi. |
| WDLP.15 | Przygotowanie procedur wnioskowania o nową politykę DLP, objęcie ochroną nowej grupy danych, obsługi zdarzenia i obsługi incydentu bezpieczeństwa związanego z wyciekiem danych, procedurę eskalacji na wypadek braku aktywności osób odpowiedzialnych za obsługę zdarzenia/incydentu, cyklicznego tworzenie aktualizacji sygnatur chronionych danych.  |
| WDLP.16 | Opracowanie szablonu raportów z incydentów (ilość otwartych/zamkniętych incydentów) w zadanym czasie z podziałem na rodzaj incydentów (dane osobowe, tajemnica przedsiębiorstwa itp.). |
| WDLP.17 | System musi być zintegrowany z usługą katalogową Zamawiającego (Microsoft Active Directory) co najmniej w zakresie:* + - 1. przypisywanie użytkowników i grup jako autoryzowanych nadawców i odbiorców monitorowanych informacji,
			2. przypisanie użytkowników do ról zarządzających takich jak Administrator, Operator incydentów DLP, Manager Incydentów CPPC,

wyświetlanie szczegółów dotyczących użytkownika w ramach incydentu związanego z jego aktywnością, np. powinno być możliwe zdefiniowanie/wyświetlenie informacji o zwierzchniku użytkownika. |
| WDLP.18 | Wykonawca dokona instalacji i integracji systemu DLP z:* Serwer usług katalogowych Active Directory (minimum Windows Server 2012 R2-32/64-bit lub nowszy) co najmniej w zakresie:
	+ przypisywanie użytkowników i grup jako autoryzowanych nadawców i odbiorców monitorowanych informacji,
	+ przypisanie użytkowników do ról zarządzających takich jak Administrator, Operator incydentów DLP, Manager Incydentów CPPC,
	+ wyświetlanie szczegółów dotyczących użytkownika w ramach incydentu związanego z jego aktywnością, np. powinno być możliwe zdefiniowanie/wyświetlenie informacji o zwierzchniku użytkownika,
* 180 stacji roboczych (minimum Windows 7)
* Serwer wirtualny udostępniony przez Zamawiającego (minimum Windows Server 2012 R2-32/64-bit lub nowszy),
* instancją bazy danych obsługującą System DLP, którą Wykonawca stworzy na udostępnionym serwerze wirtualnym Zamawiającego (Jeśli Wykonawca zamierza użyć bazy MS SQL Server, to Zamawiający udostępni Wykonawcy niezbędną instancję bazy danych, hostowaną na centralnym serwerze bazodanowy, będącym w posiadaniu Zamawiającego),
* systemem SIEM zamawiającego opartego o ELK.
 |
| WDLP.19 | Ochroną danych muszą zostać objęte następujące elementy:* Ruch sieciowy wychodzący na zewnątrz
* Stacje robocze użytkowników
* Serwer plików Windows
 |

## Wymaganie dotyczące dostrajania systemu DLP

|  |  |
| --- | --- |
| **Kod wymagania** | **Opis wymagania** |
| WDS.01 |  Wykonawca zapewni wsparcie przez okres 90 dni kalendarzowych, w procesie dostrajania systemu DLP, poprzez wsparcie operatorów DLP Zamawiającego w zakresie obsługi incydentów. |
|  | Wykonawca zapewni wsparcie przez okres 90 dni kalendarzowych, w procesie dostrajania systemu DLP poprzez wsparcie administratorów systemu DLP Zamawiającego. |
| WDS.02 | Dostrajanie systemu będzie obejmowało, analizę incydentów oraz optymalizację polityk wdrożonych we wcześniejszych etapach a jeśli to konieczne tworzenie i usuwanie istniejących. |
| WDS.03 | Celem dostrajania systemu będzie dążenie do ograniczenia fałszywych incydentów (false-positive) otrzymywanych przez operatorów DLP i optymalizacja pracy operatorów, dodawanie i usuwanie reguł, zgodnie z pojawiającymi się potrzebami w okresie dostrajania systemu. |
| WDS.04 | Aktualizacja procedur i dokumentacji niezbędnych po zmianach w systemach. |
| WDS.05 | Wydawanie rekomendacji w zakresie poprawy poziomu bezpieczeństwa informacji w ramach systemu DLP.  |

## Wymagania dotyczące szkoleń użytkowników

W ramach realizacji przedmiotu zamówienia Wykonawca przeprowadzi szkolenia dla użytkowników CPPC.

|  |  |
| --- | --- |
| **Kod wymagania** | **Opis wymagania** |
| SZK.01 | Wykonawca przeprowadzi warsztat dla 3 administratorów Systemu DLP w wymiarze łącznym nie mniejszym niż 24 godziny robocze, gwarantującym przekazanie wiedzy niezbędnej do samodzielnego administrowania całym środowiskiem DLP. |
| SZK.02 | Wykonawca przeprowadzi warsztat dla 2 operatorów Systemu DLP w wymiarze łącznym nie mniejszym niż 24 godziny robocze, gwarantującym przekazanie wiedzy niezbędnej do samodzielnej obsługi incydentów, tworzenia reguł polityki w systemie DLP. |
| SZK.03 | Wykonawca przeprowadzi szkolenie w siedzibie CPPC dla wszystkich pracowników (maximum 180 osób) w minimum 3 terminach oraz przygotuje dokumentację elektroniczną do samodzielnej nauki. Szkolenie nie może być krótsze niż 2 godziny. |
| SZK.04 | Wykonawca opracuje materiały szkoleniowe dla uczestników wyżej wymienionych szkoleń. |

## Materiały szkoleniowe

W ramach realizacji przedmiotu zamówienia Wykonawca dostarczy materiały szkoleniowe spełniające następujące wymagania:

|  |  |
| --- | --- |
| **Kod wymagania** | **Opis wymagania** |
| SZKDOK.01 | Wykonawca dostarczy materiały szkoleniowe dla użytkowników systemu DLP (Administratorów, Operatorów, użytkowników końcowych) wraz z licencją do dowolnego wykorzystania, kopiowania, modyfikowania i rozpowszechniania w ramach potrzeb Zamawiającego. |
| SZKDOK.02 | Dostarczone materiały szkoleniowe muszą być w języku w polskim i muszą zawierać treść opisaną w jasny i zrozumiały dla odbiorcy. |
| SZKDOK.03 | Dostarczone materiały szkoleniowe muszą być dostępne w wersji elektronicznej umożlwiającej publikację w Intranecie Zamawiającego w postaci pliku MS Word. |
| SZKDOK.04 | Wymagane jest, aby w ramach dostarczonych materiałów szkoleniowych Wykonawca przekazał Zamawiającemu pliki źródłowe zastosowanych w niej obrazów, w tym m.in. schematów, rysunków, topologii oraz wykresów, w formacie niezabezpieczonym i edytowalnym.  |
| SZKDOK.05 | Materiały szkoleniowe muszą obejmować tematykę:* Zasad zapobiegania wyciekom informacji, zgodnie z polityką systemu DLP,
* Instrukcje postępowania dla użytkownika końcowego systemu DLP dla wszystkich możliwych przypadków pojawiających się monitów w ramach systemu DLP,
* Instrukcję postępowania z zaszyfrowanymi dokumentami przez system DLP
* Instrukcje zarządzania i konfigurowania systemem DLP
 |
| SZKDOK.06 | Cała Dokumentacja, podlega akceptacji Zamawiającego i musi być dostarczona w języku polskim, w wersji elektronicznej w niezabezpieczonym/edytowalnym formacie MS Word i niezabezpieczonym formacie PDF (na płycie CD/DVD lub innym równoważnym nośniku danych) i drukowanej, co najmniej w 1 egzemplarzu  |

## Dokumentacja

W ramach realizacji przedmiotu zamówienia Wykonawca dostarczy dokumentację spełniającą następujące wymagania:

|  |  |
| --- | --- |
| **Kod wymagania** | **Opis wymagania** |
| DOK.02 | Wykonanie dokumentacji systemu DLP. Wykonawca opracuje dokumentację powykonawczą systemu DLP zawierającą:1. Opis ogólny systemu DLP wraz z opisem architektury logicznej systemu i graficzną prezentacją połączeń,
2. Schematy uwzględniające przepływ danych pomiędzy elementami systemu do ochrony przed wyciekiem danych. Schematy muszą uwzględniać wszystkie systemy Zamawiającego,
3. Opis funkcjonowania dostarczonych elementów systemu DLP,
4. Specyfikację techniczną,
5. Inwentaryzację urządzeń i oprogramowania systemu DLP wchodzących w skład całego systemu do ochrony
6. konfigurację systemu do ochrony, opis zaimplementowanych polityk,
7. politykę dla systemu z uwzględniającą wymagania RODO, ze wskazaniem jakie dane są chronione i zgodnie z tym co wymaga Zamawiający (PESEL itd.)
8. procedurę cyklicznego tworzenia/uaktualniania sygnatur chronionych danych z plików znajdujących się na serwerze plików (minimum Windows Server 2012 R2-32/64-bit lub nowszy).
9. proces obsługi incydentów bezpieczeństwa związanych z wyciekiem danych.

Proces musi zawierać następujące elementy:* + Procedurę postępowania w przypadku wykrycia incydentu,
	+ Procedurę eskalacji w przypadku braku aktywności osób odpowiedzialnych za obsługę incydentów,
	+ Szablon raportu/raportów zawierających:
		- Ilość otwartych incydentów w zadanym przedziale czasu
		- Ilość zamkniętych incydentów w zadanym przedziale czasu
1. Opis procedur dot. backupu systemu DLP oraz archiwizacji danych, procedurę odtwarzania systemu i bazy zdarzeń/incydentów wraz z opisem odtwarzaniem systemu, bazy i incydentów,
2. Instrukcje instalacyjne i instrukcje obsługi dla administratora systemu do ochrony przed wyciekiem danych,
3. Instrukcje obsługi dla użytkowników systemu DLP (administratora, operatora konsoli do obsługi incydentów),
 |
| DOK.03 | W okresie gwarancji/dostrajania systemów, Wykonawca zobowiązany jest do usuwania wszelkich błędów merytorycznych w Dokumentacji powykonawczej oraz nanoszenia poprawek związanych z dostosowywaniem Systemu do potrzeb Zamawiającego w terminie nie dłuższym niż **20 dni** roboczych od dnia ich zgłoszenia przez Zamawiającego. Poprawiona Dokumentacja powinna być dostarczona Zamawiającemu w formie elektronicznej w języku polskim.  |
| DOK.04 | Wymagane jest, aby w ramach Dokumentacji przekazał Zamawiającemu pliki źródłowe zastosowanych w niej obrazów, w tym m.in. schematów, rysunków, topologii oraz wykresów, w formacie niezabezpieczonym i edytowalnym. |
| DOK.05 | Cała Dokumentacja, podlega akceptacji Zamawiającego i musi być dostarczona w języku polskim, w wersji elektronicznej w niezabezpieczonym/edytowalnym formacie MS Word i niezabezpieczonym formacie PDF (na płycie CD/DVD lub innym równoważnym nośniku danych) i drukowanej, co najmniej w 1 egzemplarzu (dopuszcza się inne formaty zapisu dokumentacji np. diagramy UML lub formaty wektorowe jak DWG, DXF, należy jednak dołączyć przeglądarkę obsługującą wykorzystane formaty). Diagramy UML sporządzone za pomocą narzędzi CASE muszą być dostarczone w formacie EAP. Dostarczone wykresy Gantta muszą być dostarczone w formacie MPP lub w formacie XLS umożliwiającym import do MS Project. |
| DOK.06 | Zamawiający wymaga, aby wszystkie dokumenty tworzone w ramach realizacji przedsięwzięcia charakteryzowały się wysoką jakością, na którą będą miały wpływ, takie czynniki jak:* Struktura dokumentu, rozumiana jako podział danego dokumentu na rozdziały, podrozdziały i sekcje, w czytelny i zrozumiały sposób.
* Zachowanie standardów, w tym notacji UML, a także sposób pisania, rozumianych jako zachowanie spójnej struktury, formy i sposobu pisania dla poszczególnych dokumentów oraz fragmentów tego samego dokumentu.
* Zachowanie standardów Zamawiającego w zakresie oznaczeń dokumentów wersjonowania, metryk.
* Kompletność dokumentu rozumiana jako pełne, bez wyraźnych, ewidentnych braków przedstawienie omawianego problemu obejmujące całość z danego zakresu rozpatrywanego zagadnienia.
* Spójność i niesprzeczność dokumentu rozumianych jako zapewnienie wzajemnej zgodności pomiędzy wszystkimi rodzajami informacji umieszczonymi w dokumencie, jak i brak logicznych sprzeczności pomiędzy informacjami zawartymi we wszystkich przekazanych dokumentach oraz we fragmentach tego samego dokumentu.
 |
| DOK.07 | Dostarczona dokumentacja oraz materiały szkoleniowe muszą być w języku w polskim. |
| DOK.08 | Wykonawca dostarczy dokumentację w wersji elektronicznej na płycie CD (1 sztuka) oraz w wersji papierowej (1 egzemplarz). |

# WYMAGANIA W ZAKRESIE OZNAKOWANIA DOKUMENTACJI

Minimalne wymagania w zakresie oznakowania Dokumentacji.

|  |  |
| --- | --- |
| **Kod wymagania** | **Opis wymagania** |
| WOZN.1 | Wykonawca zobowiązany jest do:* Oznakowania dokumentacji, którą wytworzy w ramach realizowanej Umowy;
* Oznakowania nośników Oprogramowania.

Przez oznakowanie rozumie się: przygotowanie projektu graficznego oznakowanie dokumentacji zgodnego z wymaganiami Programu Operacyjnego Polska Cyfrowa. |

# GWARANCJE, WYMAGANIA PRAWNE i INNE WYMAGANE PARAMETRY TECHNICZO-UŻYTKOWE

|  |  |
| --- | --- |
| **Kod wymagania** | **Opis wymagania** |
| GWAR.01 | Systemy muszą pochodzić z legalnego kanału dystrybucyjnego producenta na rynek UE. |
| GWAR.02 | Wsparcie producenta systemu DLP oraz systemu Klasyfikacji musi być zapewnione przez cały okres obowiązywania umowy. W ramach wsparcia należy zapewnić dostęp do aktualizacji oprogramowania.  |
| GWAR.03 | Wsparcie Wykonawcy dla systemu DLP oraz systemu Klasyfikacji musi być zapewnione przez cały okres trwania umowy. Wsparcie Wykonawcy musi być realizowane w języku polskim. W ramach wsparcia zgłoszenia będą realizowane za pomocą systemu informatycznego Wykonawcy i/ lub telefonicznie – w dni robocze w godzinach 9-17. Wykonawca w ramach wsparcia zobowiązany jest również do udzielenia pomocy Zamawiającemu w usuwaniu problemów w bieżącej eksploatacji systemów, wsparcia i konsultacji w rozwoju systemu związanego z tworzeniem kolejnych polityk ochrony danych. |
| GWAR.04 | Wykonawca musi zagwarantować następujące czasy naprawy systemu DLP oraz systemu Klasyfikacji, licząc od momentu zgłoszenia przez Zamawiającego:a) **24 godziny** w przypadku Awarii systemu DLP klasyfikacji (jako Awarię Zamawiający definiuje niedostępność Systemu lub awarię Systemu, która uniemożliwia korzystanie ze stacji roboczych, na których jest zainstalowany agent; b) **48 godzin** w przypadku Błędu w Systemie (jako Błąd w systemie Zamawiający definiuje nieprawidłowe działanie Systemu lub jego komponentów, które uniemożliwia lub ogranicza prawidłowe działanie aplikacji na stacjach roboczych u Zamawiającego lub awarię systemu uniemożliwiającą zarządzanie systemem DLP i/lub systemem Klasyfikacji). |