Samodzielny Publiczny Zakład Opieki Zdrowotnej
Wojewódzki Szpital Specjalistyczny nr 4 w Bytomiu
Aleja Legionów 10, 41-902 Bytom, NIP 626-25-10-567, REGON 000296271
tel. +48 323 964 500, e-mail: szpital@szpital4.bytom.pl, www.wss4.pl

Załącznik nr 2G do SWZ

OPIS PRZEDMIOTU ZAMÓWIENIA

1. DZIAŁANIE

Projekt	382	Fundusz Przeciwdziałania COVID-19 działań w celu do podniesienia poziomu bezpieczeństwa systemów teleinformatycznych WSS4 w Bytomiu
Postępowanie	104	Zakup sprzętu komputerowego: sprzęt komputerowy dostawa i wdrożenie systemu DLP
Element	101	Opis przedmiotu zamówienia
Wersja	1	2022-10-06

2. OPIS

Dostawa i wdrożenie systemu DLP

Wykonawca dostarczy licencję minimum 3-letnią na użytkowane oprogramowania wraz z minimum rocznym wsparciem serwisowym i dostępnością aktualizacji.

Specyfikacja techniczna Systemu DLP (zabezpieczania danych przed wyciekiem)

Niniejszy dokument definiuje wymagania techniczne systemu DLP, zapewniającego kontrolę m.in. nad urządzeniami peryferyjnymi, w tym szczególnie urządzeniami podłączanymi poprzez porty USB oraz kontrolę poufnych danych wysyłanych poza sieć firmową, oferując równocześnie funkcjonalności szczegółowego raportowania rejestrowanych zdarzeń.

2.1 Parametry techniczno-funkcjonalne

1 System musi wykrywać zagrożenia związane z utratą, wyciekiem lub kradzieżą danych generowanych przez kontrolowane urządzenia, przenośne pamięci masowe, porty peryferyjne. Rozwiązanie musi zapewniać ochronę danych będących w ruchu, filtrować poufne dane organizacji, które mogą być przesyłane poza sieć wewnętrzną poprzez różne punkty wyjścia, takie jak: przeglądarki, emaile, usługi chmurowe, media społecznościowe.

1 System musi umożliwiać administratorom IT zarządzanie wszystkimi komputerami w sieci (Windows, Mac OS X i Linux) ze scentralizowanej, webowej konsoli zarządzania. Lokalny agent musi być zainstalowany na każdym chronionym komputerze.

2 System musi mieć architekturę klient-serwer i być dostępnym w trzech wariantach:
- a urządzenie wirtualne (virtual appliance) minimum w formatach:

Vmware Workstation, Vmware Player, Vmware vSphere (ESXi), Vmware Fusion, Oracle VirtualBox, Parallels Desktop Mac. Microsoft Hyper-V Server 2008-2012, Citrix XenServer (formaty plików maszyn wirtualnych: .VMX, .OVF, .OVA, .XVA, .VHD, .PVM), wstępnie skonfigurowanych przez producenta,
- b urządzenie sprzętowe (hardware appliance), w formie gotowego sprzętu z dedykowanymi licencjami i akcesoriami, który można zamontować w szafie rack (19 cali).
- c obraz wirtualny, dostosowany do implementacji w środowisku chmurowym (azure, google cloud, amazon)

3 Klient musi być dostępny minimum dla następujących rodzin systemów operacyjnych: Windows, Mac OS X, Linux.

Szczegółowy wykaz minimalnych wymagań w zakresie wspieranych wersji systemów operacyjnych:
- a Windows (32/64 bitowy): Windows 11, Windows 10, Windows 8, Windows 7, Windows Server 2019, Windows Server 2016, Windows Server 2012, Windows Server 2008, Windows 2003,
- b Mac: Mac OS 12.0, Mac OS 11.0, Mac OS 10.15, Mac OS 10.14, Mac OS 10.13, Mac OS 10.12, Mac OS X 10.11, Mac OS X 10.10, Mac OS X 10.9, Mac OS X 10.8, Mac OS X 10.7
- c Linux: Ubuntu 14.04, Ubuntu 16.04, Ubuntu 18.04, OpenSUSE/SUSE 12.1 – 12.4, CentOS /RedHat 7.0+, CentOS/RedHat 6.0+, Fedora 27 oraz 29, Debian 9.8, Mint 18.x, Oracle 7.4+

4 Komunikacja między serwerem a klientem musi odbywać się za pośrednictwem bezpiecznego połączenia (https) na dowolnie konfigurowanym porcie.

5 Rozwiązanie musi zapewniać integrację z Active Directory (AD), co oznacza, że elementy składowe AD (w tym szczególnie: jednostki organizacyjne, grupy, komputery, użytkownicy) mogą być importowane na serwer systemu DLP. Dodatkowo wymagana jest możliwość włączenia mechanizmu synchronizacji zmian z AD. Instalacja agenta na wszystkich komputerach w sieci musi być możliwa w sposób zautomatyzowany, bez angażowania użytkownika stacji końcowych.

6 Rozwiązanie musi zapewniać dostęp do systemu DLP zarówno z sieci wewnętrznej lub zewnętrznej. Administrator musi mieć możliwość połączenia się za pomocą nazwy użytkownika i hasła z dowolnego komputera w sieci wewnętrznej lub przez Internet, jeśli rozwiązanie zostanie wdrożone w wariancie z zewnętrznym adresem IP.

7 Interfejs zarządzający rozwiązania musi być dostępny minimum w języku polskim i angielskim.

8 Rozwiązanie musi posiadać co najmniej dwa poziomy uprawnień dla kont administratorów:
- a konto administratora (root) z pełnymi uprawnieniami do zarządzania systemem DLP,
- b konta administratorów z ograniczonymi uprawnieniami.

9 System musi mieć możliwość nadawania odpowiednich ról dla administratorów, które ograniczą ich możliwości zarządzania systemem,

10 Rozwiązanie musi pozwalać na utworzenie oddzielnych zestawów konfiguracji polityk bezpieczeństwa, dedykowanych jednostkom organizacyjnym danej firmy, łącznie z możliwością utworzenia konta administratora delegowanego do zarządzania danym modułem.

11 Administrator systemu DLP musi mieć możliwość zdefiniowania minimum następujących akcji dla przenośnych pamięci masowych używanych wewnątrz organizacji:
   a blokuj,
   b zezwól,
   c tylko do odczytu.
   d pozwól gdy urządzenie jest szyfrowane (dostęp tylko do części szyfrowanej)
12 Uprawnienia muszą być przydzielane co najmniej na następujących poziomach:
   a globalnie (ustawienia mają zastosowanie do wszystkich komputerów chronionych systemem DLP),
   b poziom grupy (ustawienia odnoszą się do komputerów i użytkowników w grupie),
   c poziom komputera (ważny dla jednego komputera),
   d poziom użytkownika (ustawienia dostępne dla pojedynczego użytkownika),
   e poziom urządzenia (ustawienia dostępne dla określonego urządzenia przenośnego).

Administrator musi mieć możliwość zmiany priorytetu ustawień dla poziomu komputera lub użytkownika.

13 System musi identyfikować i zarządzać co najmniej wymienionymi poniżej urządzeniami oraz portami peryferyjnymi, z następującymi prawami:
   a urządzenia pamięci USB - Odmów dostępu / Zezwalaj na dostęp / Tylko do odczytu / Zezwalaj na dostęp, jeśli urządzenie jest zaufane / Zezwalaj na dostęp, jeśli urządzenie jest zaufane a jeśli nie jest zaufane – tylko do odczytu
   b wewnętrzny napęd CD/ DVD RW - Odmów dostępu / Zezwalaj na dostęp / Tylko do odczytu,
   c wewnętrzny czytnik kart pamięci - Odmów dostępu / Zezwalaj na dostęp / Tylko do odczytu,
   d wewnętrzny napęd dyskietek - Odmów dostępu / Zezwalaj na dostęp / Tylko do odczytu,
   e drukarki lokalne - Odmów dostępu / Zezwalaj na dostęp,
   f przenośne urządzenia z systemem Windows - Odmów dostępu / Zezwalaj na dostęp
   g aparat cyfrowy - Odmów dostępu / Zezwalaj na dostęp,
   h BlackBerry - Odmów dostępu / Zezwalaj na dostęp,
   i SmartPhone (Windows CE) - Odmów dostępu / Zezwalaj na dostęp,
   j SmartPhone (Symbian) - Odmów dostępu / Zezwalaj na dostęp,
   k Android Smartphone (Media Transfer Protocol) - Odmów dostępu / Zezwalaj na dostęp,
   l iPhone - Odmów dostępu / Zezwalaj na dostęp,
   m iPad - Odmów dostępu / Zezwalaj na dostęp,
   n iPod - Odmów dostępu / Zezwalaj na dostęp,
   o kamera internetowa - Odmów dostępu / Zezwalaj na dostęp,
   p kontroler Serial ATA - Odmów dostępu / Zezwalaj na dostęp,
   q WiFi - Odmów dostępu / Zezwalaj na dostęp / Blokuj Wi-Fi, jeśli jest dostępna sieć przewodowa,
   r Bluetooth - Odmów dostępu / Zezwalaj na dostęp,
   s FireWire - Odmów dostępu / Zezwalaj na dostęp / Tylko do odczytu,
   t port szeregowy - Odmów dostępu / Zezwalaj na dostęp,
   u port równoległy (LPT) - Odmów dostępu / Zezwalaj na dostęp,
   v PCMCIA - Odmów dostępu / Zezwalaj na dostęp / Tylko do odczytu,
   w MTD - Odmów dostępu / Zezwalaj na dostęp / Tylko do odczytu,
   x SCSI - Odmów dostępu / Zezwalaj na dostęp / Tylko do odczytu,
   y napęd ZIP - Odmów dostępu / Zezwalaj na dostęp / Tylko do odczytu,
   z Thunderbolt - Odmów dostępu / Zezwalaj na dostęp / Tylko do odczytu,
   aa udziały sieciowe - Odmów dostępu / Zezwalaj na dostęp,
   bb port podczerwieni - Odmów dostępu / Zezwalaj na dostęp,
   cc Thin Client Storage (RDP Storage) - Odmów dostępu / Zezwalaj na dostęp / Tylko do odczytu,
   dd dodatkowa klawiatura - Odmów dostępu / Zezwalaj na dostęp,
   ee modem USB - Odmów dostępu / Zezwalaj na dostęp / blokuj w przypadku obecności sieci przewodowej,
   ff Nieznane urządzenie - Odmów dostępu / Zezwalaj na dostęp.
14 Administrator musi mieć możliwość monitorowania, które pliki zostały skopiowane przez użytkowników (pracowników) i na jakie urządzenia. System musi pozwalać na generowanie raportów obejmujących co najmniej następujące informacje:
   a jaki plik został przesłany / usunięty / z edytowany
   b typ i rozmiar,
   c użytkownik,
   d nazwa komputera i adres IP z którego dokonano transferu,
   e nazwa urządzenia przenośnego wraz z numerem seryjnym (jeśli dostępny),
   f data i godzina przekazania, funkcje skrótu pliku.
15 System musi pozwalać na eksportowanie raportów jako pliki CSV, PDF, Excel do lokalizacji określonej przez administratora.
16 Administrator musi mieć możliwość włączenia lub wyłączenia powiadomień dla użytkowników o zablokowanych akcjach na stacjach roboczych
17 Administrator musi mieć możliwość ustalenia godzin w jakich będą obowiązywały polityki firmowe.
18 Administrator musi mieć możliwość ustalenia sieci LAN w jakich będą obowiązywały polityki firmowe.
19 Administrator musi mieć możliwość ustalenia limitu wielkości lub ilości przesyłanych plików w danej jednostce czasu.
20 Rozwiązanie musi pozwalać administratorowi na kontrolowanie przesyłania plików za pośrednictwem minimum następujących aplikacji internetowych:
   a przeglądarki internetowe: Internet Explorer, Edge, Chrome, Mozilla Firefox, Opera, Safari, AOL Desktop 9.6, Aurora Firefox, Brave, Adobe Flash Player, Tor, Camino, iCab, OmniWeb, Sleipnir, K-Meleon, SeaMonkey, Maxthon, FrontMotion Firefox, Pale Moon, Swing, Torch, Whale
   b klienci pocztowi: Outlook, Outlook (Body), Mozilla Thunderbird, Mozilla Thunderbird (Body), IBM Lotus Notes v.6.5-v.9.0, IBM Lotus Notes v.6.5-v.9.0 (Body), Geary, Evolution, Claws Mail, Sylpheed, Balsa Mail Client, Windows Live Mail, GroupWise Client, Foxmail, SeaMonkey Mail, Zimbra Desktop

Mail, Eudora, eM Client, Sparrow, GyazMail, PowerMail, AirMail Beta, Sparrow Lite, Postbox, Mail, Outlook Express, Windows Mail, AOL Mail, Courier, Opera Mail,

c Komunikatory internetowe: ICQ, AIM, Skype, Windows Live Messenger, Yahoo Messenger, Gaim, Pidgin, Trillian, NateOn Messenger, Spark, Telegram Desktop, Messages, Audium, Line, Hall, OpenTalk, TurnoIRC, WinSent Messenger, xChat, TweetDeck, Pink Notes Plus, Google Talk, Thwirl, QQ International, mIRC, MySpace IM, Duam MyPeople, Kakao Talk, Chit Chat for Facebook, eBuddy, Facebook Messenger, fTalk, Microsoft Communicator 2007, LingoWare, Lan Chat Enterprise, My Chat, Nimbuzz, ooVoo, Microsoft Link, Mail.Ru Agent, Slack, Psi+, Viber, Discord, Zalo, WhatsApp Desktop

d Usługi chmurowe / Udostępnianie plików: Google Drive Client, iCloud Client, uTorrent, BitComet, Daum Cloud, Kt Olleh uCloud, Azureus, Box Sync, Sugar Sync, Picasa, Amazon Drive, iBooks Author, MediaFire Client, Novell Filr Client, AirDrop, Transmission, Morpheus, FileCloud Sync Client, OneDrive (Skydrive) Client, Lime Wire, FTP Command, BitTorrent, ownCLoud Client, Pogoplug Backup, Shareaza, Pruna P2P, SendSpace, DC ++, Dropbox, eMule, Evernote, Kazaa, Android File Transfer, GitHub Client, MEGA, Yandex Desk, KRDC, qBittorrent, Linex DC++, Webhard, Send Anywhere, SideSync

e Media społecznościowe / Inne: Windows Apps, EasyLock, Team Viewer, Windows DVD Maker, Total Commander, ALFTP, LogMeIn Pro, iTunes, FileZilla, SCP, total Commander 64 bit, Sony Ericsson PC Companion, InfraRecorder CD-DVD, HTC Sync for Android, GoToMeeting, Nokia PC Suite 2011 Video Transfer, Nokia PC Suite 2011 Image Store, Nokia PC Suite 2011, Nokia PC Suite 2008 Main, Nokia PC Suite 2008, Zoom, Station, VNC, Wormhole Switch DSS, Samsung DeX, Samsung Kies, PowerShell, iMazing, CuteFTP,

21 Rozwiązanie musi pozwalać administratorom na kontrolowanie przesyłania plików za pomocą funkcjonalności filtrów działających minimum w oparciu o:
   a typ pliku,
   b wykryty kod źródłowy,
   c wstępnie zdefiniowaną zawartość,
   d spersonalizowaną treść,
   e nazwę pliku,
   f wyrażenia regularne.

22 Filtry bazujące na rozszerzeniach plików muszą pozwalać na wykrywanie minimum poniższych rodzajów plików:
   a pliki graficzne: JPEG, PNG, GIF, ICO, BMP, TIFF, CGM, Corel Photo – Paint, CorelDraw, DJV, EPS, Adobe Illustrator, Adobe inDesign, BPF, PSD,
   b pliki pakietu Microsoft Office: Word, Excel, PowerPoint, PDF, Infopath, Outlook, Publisher, iWork files, Office 2007+/password,
   c archiwa plików: ZIP, ZIP/password, 7z, RAR, ACE, TAR, XZ, .XAR, ACE/password, RAR/password, BZ2, GZ,
   d pliki multimedialne: Mov, Mp3, M4a, mp4, Wav, Wma, Avi, Aif, M3u,
   e pozostałe pliki: Text files, DRM Files, Exe, sys, dll, Fasoo Files, Journal files, so, unindetified, .accdb, Bdf, Csr, DTA, EPP_ENCRYPTED FILES, FDL, NASCA DRM, P12, SgWgc, SID, SSD, VMDK, Xia, XML / DTD, FDL, HUE, RODE, SEGD, SEGY,
   f CAD files: AutoCAD, I-DEAS 3D CAD, IGS, Pro-E CAD, Prt, REVIT, SMG, SOLID EDGE, SolidWorks, STL, WRL, XDL, CATIA,

Na życzenie użytkownika systemu DLP producent rozwiązania powinien dodać niezbędne, brakujące typy plików.

23 System posiada możliwość kontroli wysyłki kodu źródłowego, wraz z zaimplementowanym mechanizmem uczenia maszynowego, który pozwala na zmniejszenie ilości false-positivów wraz z tokiem nauki,

24 System musi posiadać predefiniowane polityki, które będą zgodne co najmniej z regulacjami:
   a HIPAA
   b PCI
   c GDPR / RODO

25 System musi posiadać możliwość blokowania dostępu do wybranych domen i/ lub adresów URL

26 System musi posiadać możliwość zezwolenia na dostęp i wysyłania plików do wybranych domen i/lub adresów URL

27 System musi posiadać sprawdzanie danych aplikacji na niestandardowych portach, zdefiniowanych przez administratora.

28 System DLP musi pozwalać na zdefiniowanie co najmniej trzech akcji związanej z zadziałaniem polityki kontrolowania plików:
   a tylko raportuj,
   b tylko blokuj,
   c blokuj i raportuj,
   d na wszystkie transfery danych, które zawierają istotne dane (zgodnie ze zdefiniowanymi filtrami).

29 Predefiniowane filtry zawartości muszą umożliwiać administratorom zautomatyzowane zarządzanie transferem plików zawierających dane wrażliwe, rozumiane jako co najmniej:
   a numery kart kredytowych,
   b numery IBAN,
   c numery SWIFT,
   d numery PESEL,
   e adresy korespondencyjne,
   f adresy e-mail,
   g numery telefonów,
   h numery dowodów osobistych
   i numery NIP
   j Adresy protokołów internetowych w wersji 4 i 6

30 System musi umożliwiać tworzenie niestandardowych filtrów treści dających administratorom możliwość zarządzania transferem plików na podstawie słów kluczowych.

31 System musi umożliwiać zarządzanie transferem plików zawierających dane rekurencyjne, na podstawie definiowalnych przez administratora filtrów korzystających z wyrażeń regularnych.

32 W przypadku wykrycia kopiowania pliku z wrażliwymi danymi rozwiązanie musi pozwalać na utworzenia jego duplikatu na serwerze systemu DLP (tzw. funkcjonalność „File Shadow").

33 Rozwiązanie musi posiadać także funkcjonalność śledzenia i zachowywania informacji o ruchu wszystkich plików przenoszonych przez dowolnego użytkownika podłączonego do chronionego komputera.

34 System musi posiadać zintegrowany moduł automatycznego szyfrowania plików przenoszonych na urządzenia przenośne.
35 Rozwiązanie musi mieć możliwość wysyłania w czasie rzeczywistym alertów przez e-mail do administratorów, gdy wykryte zostanie predefiniowane zdarzenie (np. możliwy wyciek danych).
36 System musi posiadać możliwość tworzenia własnych okien, aby powiadamiać użytkownika o wykonywanej akcji.
37 Użytkownik końcowy musi mieć możliwość zaakceptowania powiadomienia, w celu przesłania danego pliku. (Jeżeli zostało to ustawione w polityce)
38 Rozwiązanie musi być w stanie dostarczyć statystyki i wykresy dotyczące korzystania z urządzeń przenośnych i transferu plików w sieci.
39 Rozwiązanie musi zapewniać ciągłą ochronę komputera, nawet jeśli jest odłączony lub usunięty z sieci wewnętrznej. Ustawienia polityk ochrony muszą pozostać aktywne, nawet jeśli komputer nie ma połączenia z serwerem systemu DLP. Wygenerowane w tym czasie logi i raporty muszą być przechowywane lokalnie na danym komputerze a przy ponownym połączeniu z serwerem muszą zostać do niego przesłane.
40 Oprogramowanie agentów systemu DLP na stacjach końcowych musi być chroniony hasłem zapobiegającym odinstalowaniu agenta.
41 Rozwiązanie musi pozwalać administratorowi na czasowe autoryzowanie podłączenia pamięci USB do komputerów, nawet gdy komputer nie jest podłączony do serwera systemu DLP.
42 Rozwiązanie musi pozwalać administratorowi na wymuszenie podania powodu użycia czasowej autoryzacji w celu podłączenia pamięci USB do komputerów.
43 System musi pozwalać administratorom dostosować interwał komunikacji między agentami a serwerem (czas w którym klient wysyła logi i raporty do serwera).
44 System musi pozwalać administratorom zdefiniować "białą listę" plików, które można kopiować na autoryzowane urządzenia.
45 System musi pozwalać administratorom na zdefiniowanie "białej listy" adresów URL i domen, do których możliwe będzie przesyłanie plików.
46 Rozwiązanie musi posiadać funkcjonalność aktualizacji, umożliwiającą instalowanie najnowszych dostępnych wersji z poziomu webowej konsoli zarządzającej.
47 Webowa konsola zarządzająca musi pozwalać na:
   a zdefiniowanie, zmianę oraz kontrolę bieżących ustawień systemu DLP,
   b dostęp do raportów i danych statystycznych związanych z działaniem systemu DLP,
   c wyłączenie oraz restart systemu DLP.
48 Rozwiązanie musi pozwalać administratorom na wysyłanie wiadomości bezpośrednio do działu pomocy technicznej producenta. Wsparcie techniczne musi być oferowane co najmniej w języku angielskim.
49 System musi obsługiwać optyczne rozpoznawanie znaków (OCR).
50 System DLP musi pozwalać na integrację z zewnętrznymi rozwiązaniami SIEM, rozumianą jako możliwość przesyłania rejestrowanych zdarzeń do zewnętrznego serwera SIEM w celu ich analizy i raportowania.
51 System DLP musi mieć możliwość blokowania dostępu na dane strony internetowe, zdefiniowane przez administratora.
52 System DLP opcjonalnie musi pozwalać administratorowi na tworzenie polityki aktywnego sprawdzania/skanowania danych znajdujących się na chronionych komputerach Mac, Windows i Linux, umożliwiając egzekwowanie wewnętrznej polityki bezpieczeństwa danych firmy oraz zarządzanie ryzykiem stwarzanym przez przypadkowe lub zamierzone wycieki danych. Rozwiązanie musi umożliwiać co najmniej dwa rodzaje skanów:
   a skan początkowy (czysty): wykrywanie danych wrażliwych od zera,
   b skan przyrostowy: kontynuacja wykrywania (pomijając wcześniej zeskanowane pliki).

Administrator musi mieć możliwość zarządzania wynikami skanowania, w tym listą wszystkich komputerów, które były skanowane. Rozwiązanie (w zakresie funkcjonalności aktywnego skanowania) musi pozwalać na podjęcie minimum następujących akcji:
   a usuwanie,
   b szyfrowanie lub odszyfrowywanie plików.

Administrator musi mieć możliwość zastosowania żądanej akcji do każdego elementu indywidualnie lub do grupy wybranych elementów jednocześnie.
53 Wymagane jest aby producent zapewniał wsparcie techniczne minimum przez: telefon, e-mail, czat na żywo oraz zdalne połączenie.
54 Wymagana jest możliwość zakupu wdrożenia systemu lub godzinowego wsparcia przy implementacji,

2.2 Moduł Automatycznego Szyfrowania Pamięci Masowych USB

1 Moduł musi być dostępny na co najmniej dwóch platformach: Windows oraz Mac OS
2 Moduł musi umożliwiać ustawienie ręcznego lub automatycznego instalowania aplikacji na podłączanych urządzeniach pamięci masowych USB
3 Moduł musi obsługiwać szyfrowanie w standardzie co najmniej AES 256
4 Moduł musi umożliwić wymuszenie obecności agenta systemu DLP na stacji końcowej, w przypadku próby uruchomienia aplikacji do szyfrowania z urządzenia
5 Moduł musi umożliwić opcje automatycznych aktualizacji aplikacji do szyfrowania na urządzeniach USB
6 Moduł musi umożliwiać zdefiniowane haseł nadrzędnych przez administratora
7 Moduł musi umożliwiać administratorowi wymuszenie złożoności hasła dla użytkownika oraz dla administratora, jeśli chodzi o:
   a Długość
   b Ilość małych i dużych liter
   c Ilość cyfr
   d Ilość znaków specjalnych
   e Blokowanie następujących po sobie liter lub cyfr (np. abcdef123456)
8 Moduł musi pozwolić administratorowi ustalić okres ważności hasła użytkownika oraz hasła administratora
9 W przypadku wygaśnięcia hasła administrator musi mieć możliwość ustalenia historii haseł, na które to nie będzie możliwa zmiana
10 Moduł musi mieć możliwość ustalenia ilości błędnych prób logowania po których nastąpi blokada zawartości urządzenia przenośnego
11 Administrator musi mieć możliwość włączenia lub wyłączenia śledzenia plików kopiowanych osobno dla trybu online oraz offline
12 Administrator musi mieć możliwość wysłania wiadomości do użytkownika logującego się do aplikacji szyfrującej na danym urządzeniu
13 Administrator musi mieć możliwość zmiany hasła użytkownika w przypadku jego utraty
14 Administrator musi mieć możliwość wyczyszczenia wnętrza aplikacji w przypadku zgubienia urządzenia pamięci masowej USB
15 W przypadku wysłania złej komendy, administrator musi mieć możliwość anulowania wydanych dotąd komend

16 Administrator musi mieć możliwość nadania opisu dla konkretnej aplikacji, w celu łatwiejszej identyfikacji samej aplikacji jak i urządzenia na którym została ona zainstalowana.

3. INNE WYMAGANIA

1. Zakres prac

W ramach realizacji przedmiotu zamówienia Wykonawca:

- Dokona dostawy przedmiotu zamówienia, uruchomienie i konfigurację.
- Dokona instalacji i konfiguracji oprogramowania na serwerze
- Przeprowadzi instruktaże w zakresie użytkowania systemu dla personelu
- Przeprowadzi instruktaż w zakresie administrowania systemem
- Przekaże niezbędną dokumentacji powykonawczą
- Przekaże licencje bezterminowe, bez ograniczeń terytorialnych do oprogramowania

2. Dostawa

- Oferowane wyposażenie musi być fabrycznie nowe i nieużywane, pochodzić z bieżącej produkcji (rok produkcji – 2021/2022),
- Koszty uruchomienia, konfiguracji, przekazania licencji oraz szkolenia personelu Zamawiającego ponosi Wykonawca. Dostawa nastąpi po wcześniejszym ustaleniu terminu, w dniu roboczym, w godzinach między 8:00 a 15:00.

3. Instruktaż

Wykonawca w ramach realizacji przedmiotu zamówienia przeprowadzi instruktaż pracowników Zamawiającego z zakresu prawidłowej obsługi dostarczonego systemu wraz z urządzeniami zgodnie z wymaganiami określonymi w SWZ.

4. Wsparcie techniczne

Usługa wsparcia technicznego przez okres min. 36 miesięcy dla zapewnienia ciągłości pracy oprogramowania poprzez wykonywanie w ramach usługi działań min.:

- Konsultacje telefoniczne dotyczące instalacji i eksploatacji oprogramowania opieka techniczna nad programem
- Świadczenie usług doradztwa technicznego obejmujące w szczególności.:
  - diagnozę oprogramowania w celu wykrycia sytuacji niepożądanych, w tym w szczególności monitorowanie zdarzeń zagrażających bądź potencjalnie zagrażających bezpieczeństwu systemu i właściwa reakcja na nie.
  - sprawdzenie poprawności działania aplikacji.
  - naprawa pojawiających się usterek.
- Przyjmowanie zgłoszeń Zamawiającego przy wykorzystaniu: infolinii (bezpośredni kontakt telefoniczny z konsultantem) oraz email (zgłaszanie problemów przez Internet)
- Czas reakcji serwisu technicznego od zgłoszenia awarii nie dłuższy niż 24 godziny od chwili zgłoszenia
- Czas usunięcia awarii nie dłuższy niż 5 dni roboczych.
- Przyjmowania zgłoszeń błędnego działania oprogramowania w godzinach 8:00 – 16:00 w dni robocze
- Świadczenie usług aktualizacji oprogramowania (o ile zostanie wydana przez Producenta).

5. Gwarancja

- Okres gwarancji liczony jest od daty podpisania protokołu odbioru bez zastrzeżeń.
- Gwarancja na wykonane usługi min. 12 miesięcy maks. 60 miesięcy

6. Dokumentacja

Wykonawca wraz z dostawą przedmiotu umowy zobowiązany jest przekazać:

- Dokumentację dla użytkownika z obsługi oprogramowania w języku polskim
- Instrukcję wykonywania kopii bezpieczeństwa w języku polskim
- Instrukcja odzyskiwania danych z kopii bezpieczeństwa w języku polskim,
- Instrukcję dotycząca konfiguracji oprogramowania, w języku polskim
- Nośniki oprogramowania i dokumenty licencyjne producenta oprogramowania.