Załącznik nr 7 do SIWZ

SZCZEGÓŁÓWY OPIS PRZEDMIOTU ZAMÓWIENIA (OPZ)

Oferowane produkty muszą spełniać wszystkie parametry określone w niniejszym opisie oraz być fabrycznie nowe, oznakowane symbolem CE, pochodzić z legalnego źródła, muszą być dostarczone przez autoryzowany kanał sprzedaży producenta na terenie kraju.

Zamawiający zastrzega sobie prawo weryfikacji pochodzenia sprzętu u Producenta i w przypadku zastrzeżeń, iż dostarczony sprzęt nie pochodzi z oficjalnego kanału dystrybucyjnego lub nie jest nowy, Zamawiający będzie domagał się wymiany sprzętu na właściwy a wszelkie koszty z tym związane ponosi Oferent.

Wykonawca winien przedstawić nazwę producenta i model oferowanego sprzętu i oprogramowania w poszczególnych jego rodzajach. Wszystkie opisane parametry wymagane są wymaganiami minimalnymi. Zamawiający akceptuje rozwiązania o parametrach równoważnych lub lepszych, bez utraty funkcjonalności i wydajności.

1. Urządzenia wielofunkcyjne – 5 sztuk

1	Technologia druku	kolorowy druk laserowy, automatyczny druk dwustronny w standardzie
2	Technologia tonera	tonery CMYK
3	Szybkość druku	A4 kolor: minimum 30ppm, A4 mono: minimum 30ppm simplex/duplex
4	Czas oczekiwania na wydruk pierwszej strony kolorowej	max 7,3 sek
5	Czas oczekiwania na wydruk pierwszej strony mono	max 5,6 sek
6	Czas nagrzewania	max 20 sek.
7	Pamięć RAM	minimum 4GB
8	Dysk twardy	minimum 250 GB w standardzie z funkcją szyfrowania danych
9	Język wydruku	PCL6, PCL5e/c, PostScript3, XPS, wymagany oryginalny sterownik producenta urządzenia, interfejs sterownika druku z możliwością edytowania zakładki z ulubionymi opcjami, interfejs sterownika druku w języku polskim
10	Rozdzielczość wydruku	minimum 1200 x 1200 dpi
11	Maksymalne obciążenie miesięczne	minimum 125 000 stron miesięcznie
12	Kopiowanie wielokrotne	1-9999
13	Powiększenie	25–400 % w odstępach 0,1%, Automatyczne powiększanie
14	Funkcje kopiowania/drukowania	wstawianie rozdziałów, okładek i stron, kopia próbna (drukowana i ekranowa), druk próbny do regulacji, tryb plakatowy, powtarzanie obrazu, znak wodny, pieczętowanie, ochrona przed kopiowaniem, kopiowanie dokumentów tożsamości, bezpieczny wydruk, Pomijanie pustych stron, wydruk bannerowy, tworzenie ulotek, wstawianie obrazów

15	Pierwszy podajniki papieru	500 arkuszy (format A5 do A3), obsługiwana gramatura 52 - 256 g/m2
16	Drugi podajnik papieru	500 arkuszy (format A5 do SRA3 [320x 450mm]), obsługiwana gramatura 52 - 256 g/m2
17	Podajnik papieru ręczny	150 arkuszy, A6–SRA3, niestandardowe wymiary (szerokość 90-320mm, długość 139,7 - 1200mm), banner (297 x 1,200 mm, gramatura 160), koperty, etykiety, maksymalna obsługiwana gramatura papieru 300 g/m2
18	Dodatkowe podajniki papieru	Możliwość doposażenia o dodatkowe podajniki kaset w podstawie urządzenia
19	Podajnik oryginałów	100 arkuszy, format oryginałów A6 - A3, podajnik z funkcją jednoprzebiegowego skanowania dwustronnego,
20	Pojemność odbiorcza	minimum 250 arkuszy
21	Prędkość skanowania	Minimum 150 oryginałów na minutę w trybie kolor i monochromatycznym
22	Rodzaj modułu skanera	wbudowany jednoprzebiegowy kolorowy skaner, z wbudowanym energooszczędnym oświetleniem w technologii LED
23	Rozdzielczość skanowania	minimum 600 x 600 dpi
24	Tryby skanowania	Scan-to-USB, Scan-to-Me, Skan-to-SMB, Scan-to-Home, Scan-to-FTP, Scan-to-Box, Scan-to-USB, Scan-to-WebDAV, Scan-to-DPWS, Network TWAIN scan. Adnotacje (tekst/godzina/data) w plikach PDF; Pomijanie pustych stron. Podgląd i edycja zeskanowanych obrazów przed wysłaniem/zapisaniem.
25	Obsługiwane formaty papieru	A6–SRA3, niestandardowe wymiary (max 320 x 450 mm), banner: (210-297 x 457,3 x 1200mm,)koperty, etykiety
26	Obsługiwane formaty papieru w druku/kopiowaniu dwustronnym	A5-SRA3
27	Obsługiwana gramatura papieru	52 - 256 g/m2
28	Obsługiwana gramatura papieru w druku/kopiowaniu dwustronnym	52 - 256 g/m2
29	Interfejsy	USB 2.0, złącze Ethernet 10Base-T / 100Base-TX / 1000Base-T,
30	Obsługiwane protokoły	Ethernet, Apple Talk, TCP/IP (IPv4, IPv6), HTTP / HTTPS, SSL/TSL for HTTPS, SMB, Port 9100 (dwu-kierunkowy), IPP, LDAP, SNMP V3
31	Obsługiwane protokoły sieciowe	HTTP, TCP/IP (IPv4, IPv6), IPX/SPX (wsparcie ND), SMB (NetBEUI), LPD, IPP 1.1, SNMP
32	Wsparcie systemów operacyjnych	Windows VISTA x32/x64, Windows 7 x32/x64, Windows 8/8.1, Windows Server 2003x32/2003x64/2008x32/2008x64/2012/2012R2, Macintosh OS X 10.x, Unix/Linux/Citrix
33	Zasilanie	220-240 V, 50/60 Hz
34	Wyświetlacz	kolorowy 9-calowy pojemnościowy dotykowy wyświetlacz LCD wraz z wbudowaną animowaną pomocą dla użytkownika, z możliwością zdalnej

		obsługi panelu użytkownika przez przeglądarkę WWW. Dedykowany rysik w standardzie, do obsługi dotykowego wyświetlacza.
35	Język menu	Polski
36	Startowe materiały eksploatacyjne	Wszystkie materiały eksploatacyjne oferowane wraz z urządzeniami winny być oryginalne (sprzedawane pod marką producenta urządzeń), pełnowartościowe, o najwyższej możliwej do zrealizowania ilości wydruków.
37	Inne	Możliwość podłączenia wewnętrznego czytnika zbliżeniowych kart identyfikacyjnych oraz zewnętrznej klawiatury
38	Inne funkcje urządzenia	Wbudowana przeglądarka
39	Inne funkcje urządzenia	Obsługa Apple Airprint 1.4
40	Inne funkcje urządzenia	Wbudowana możliwość rozpoznawania polskiego tekstu OCR i skanowania do przeszukiwalnego PDF
41	Inne funkcje urządzenia	Dodatkowa szuflada na dokumenty i materiały eksploatacyjne będąca podstawą urządzenia umożliwiająca jego mobilność
42	Certyfikaty	ISO 9001, ISO 14001, Energy Star, TUV, CE
43	Czcionki wbudowane	Minimum: PCL: 80 czcionek, PostScript3: 120 czcionek
44	Gwarancja i rękojmia	minimum 24 m-ce

Urządzenie musi być dostarczone z kompletem startowym materiałów eksploatacyjnych.

2. System ochrony sieci

Minimalne wymagane parametry:

1	System zabezpieczeń musi być zbudowany w oparciu o dedykowane rozwiązania sprzętowe (tzw. appliance).
2	System zabezpieczeń musi zapewniać możliwość rozbudowy w przyszłości o kolejne urządzenie i pracę w klastrze w trybie Active-Passive.
3	Elementy systemu przenoszące ruch użytkowników musi dawać możliwość pracy w jednym z dwóch trybów: Router/NAT lub bridge.
4	System realizujący funkcję Firewall musi dysponować minimum 8 interfejsami miedzianymi Ethernet 10/100/1000.
5	System musi dysponować minimum 1 portem USB.
6	System musi umożliwiać tworzenie minimum 256 interfejsów wirtualnych definiowanych jako VLANy w oparciu o standard 802.1Q.
7	W ramach dostarczonego systemu ochrony muszą być realizowane wszystkie z poniższych funkcjonalności. Poszczególne funkcjonalności systemu bezpieczeństwa mogą być realizowane w postaci osobnych platform sprzętowych lub programowych: - Kontrola dostępu - zapora ogniowa klasy Stateful Inspection. - Ochrona przed wirusami – antywirus [AV] (dla protokołów SMTP, POP3, IMAP, HTTP, FTP, HTTPS). - Kontrola zawartości poczty – antyspam [AS] (dla protokołów SMTP, POP3, IMAP). - Poufność danych - IPSec VPN oraz SSL VPN. - Ochrona przed atakami - Intrusion Prevention System [IPS/IDS]. - Kontrola stron internetowych – Web Filter [WF]. - Kontrola pasma oraz ruchu [QoS i Traffic shaping].

	- Kontrola aplikacji oraz rozpoznawanie ruchu P2P. - Możliwość analizy ruchu szyfrowanego SSL'em.
8	Wydajność systemu Firewall minimum 8 000 Mbps.
9	W zakresie Firewall'a obsługa nie mniej niż 2 500 000 jednoczesnych połączeń oraz 60 000 nowych połączeń na sekundę.
10	Wydajność skanowania strumienia danych przy włączonych funkcjach: antywirus minimum 2 200 Mbps.
11	Wydajność ochrony przed atakami (IPS) minimum 2 500 Mbps.
12	Wydajność szyfrowania AES, nie mniej niż 1 000 Mbps.
13	W zakresie realizowanych funkcjonalności VPN, wymagane jest nie mniej niż: Tworzenie połączeń w topologii Site-to-site oraz możliwość definiowania połączeń Client-to-site. Monitorowanie stanu tuneli VPN i stałego utrzymywania ich aktywności. Obsługa mechanizmów: IPSec NAT Traversal, DPD.
14	Rozwiązanie musi zapewniać: obsługę Policy Routingu, routing statyczny i dynamiczny w oparciu o protokoły: RIP, OSPF, BGP.
15	Translacja adresów NAT adresu źródłowego i NAT adresu docelowego.
16	Polityka bezpieczeństwa systemu zabezpieczeń musi uwzględniać adresy IP, interfejsy, protokoły, usługi sieciowe, użytkowników, rejestrowanie zdarzeń oraz zarządzanie pasmem sieci (m.in. pasmo gwarantowane i priorytety).
17	System zabezpieczeń musi wspierać obsługę modemów 3G. Modemy powinny pochodzić od dowolnie wybranych producentów.
18	System zabezpieczeń musi umożliwiać tworzenie wydzielonych stref bezpieczeństwa Firewall np. DMZ.
19	System musi umożliwiać automatyczne przełączanie na inne łącze w przypadku awarii podstawowego łącza. System musi wspierać podłączenie co najmniej trzech niezależnych łącz.
20	W ramach ochrony IPS system musi: Opierać się, co najmniej na analizie protokołów i sygnatur. Baza wykrywanych ataków musi zawierać, co najmniej 4000 wpisów. Pozwalać na definiowanie własnych wyjątków lub sygnatur. Wykrywać anomalie protokołów i ruchu stanowiących podstawową ochronę przed atakami typu DoS oraz DDos. Generować alerty w przypadku prób ataków.
21	W zakresie kontroli aplikacji oraz rozpoznawania ruchu P2P wymagane jest co najmniej: Kontrola ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP. Baza rozpoznawanych aplikacji musi zawierać co najmniej 2000 wpisów. Blokowanie komunikatorów internetowych przynajmniej: Gadu-Gadu, Skype, Facebook Chat. Blokowanie mediów strumieniowych przynajmniej: YouTube, radio internetowe. Blokowanie uruchamiania aplikacji i gier w serwisie Facebook. Blokowanie aplikacji proxy przynajmniej: TOR, Ultrasurf, JAP. Blokowanie aplikacji P2P przynajmniej: BitTorrent, uTorrent, eMule.
22	W zakresie kontroli stron internetowych system musi: Zapewniać bazę filtra WWW pogrupowanych w kategorie tematyczne – minimum 40 kategorii. Administrator musi mieć możliwość nadpisywania kategorii oraz tworzenia wyjątków i reguł omijania filtra WWW. Umożliwiać definiowanie polityk dostępu do stron internetowych w oparciu o harmonogramy czasowe dla użytkowników i grup użytkowników. Wyświetlać komunikat użytkownikom wyjaśniający powód zablokowania dostępu do

	strony internetowej. Administrator musi mieć możliwość personalizacji treści komunikatu i dodania logo organizacji. Umożliwiać przydzielanie polityki QoS dla kategorii stron internetowych np. portale społecznościowe.
23	Automatyczne ściąganie sygnatur ataków, aplikacji, szczepionek antywirusowych.
24	System zabezpieczeń musi umożliwiać wykonywanie uwierzytelniania tożsamości użytkowników za pomocą nie mniej niż: Haseł statycznych i definicji użytkowników przechowywanych w lokalnej bazie systemu. Haseł statycznych i definicji użytkowników przechowywanych w bazach zgodnych z LDAP. Rozwiązanie musi umożliwiać budowę architektury uwierzytelniania typu Single Sign On w środowisku Active Directory.
25	Poszczególne elementy oferowanego systemu bezpieczeństwa muszą posiadać następujące certyfikaty: ICSA lub EAL4 – dla funkcjonalności Firewall.
26	System bezpieczeństwa musi być wyposażony w dysk twardy (minimum 120 GB) do celów lokalnego przechowywania logów i generowania raportów. Nie dopuszcza się składowania logów poza organizacją lub w chmurze.
27	System bezpieczeństwa musi zawierać moduł logowania zdarzeń i raportowania. Moduł logowania zdarzeń i raportowania może być realizowany w postaci osobnej platformy sprzętowej lub programowej. W ramach modułu raportowania system musi zapewniać: - składowanie oraz archiwizację logów, - gromadzenie informacji o zdarzeniach dotyczących ruchu Web, wykorzystywanych aplikacjach sieciowych, wykrytych: atakach sieciowych, wirusach, zablokowanych aplikacjach sieciowych oraz powiązanie ich z nazwami użytkowników, - przeglądanie archiwalnych logów przy zastosowaniu funkcji filtrujących, - generowanie i eksport raportów do plików HTML i PDF, - eksport zgromadzonych logów do zewnętrznych systemów składowania danych (długoterminowe przechowywanie danych).
28	Elementy systemu muszą mieć możliwość zarządzania lokalnego (HTTPS, SSH) jak i współpracować z dedykowanymi do centralnego zarządzania i monitorowania platformami. Komunikacja systemów zabezpieczeń z platformami zarządzania musi być realizowana z wykorzystaniem szyfrowanych protokołów.
29	W ramach zarządzania system bezpieczeństwa musi: - umożliwiać tworzenie kont administracyjnych o różnych uprawnieniach, - umożliwiać określanie złożoności polityk hasłowych dla administratorów, - wspierać SNMP, - monitorować na bieżąco stan urządzenia (obciążenie interfejsów sieciowych, CPU, pamięć RAM), - przechowywać przynajmniej dwie wersje firmware, - wykonywać automatycznie kopie zapasowe konfiguracji systemu.
30	Dostawca musi dostarczyć licencje aktywacyjne dla funkcji bezpieczeństwa: antywirus, antyspam, IPS, kontrola stron internetowych, kontrola aplikacji sieciowych na okres 36 miesięcy.
31	System bezpieczeństwa musi być objęty gwarancją i rękojmią producenta na okres 36 miesięcy
32	W okresie gwarancji czas reakcji serwisu od momentu zgłoszenia usterki w ciągu 1 dnia roboczego

Wdrożenie, szkolenie i instalacja wykonane w siedzibie zamawiającego.

3. Rozbudowa macierzy dyskowej

Rozbudowa posiadanej przez Zamawiającego macierzy dyskowej HP 3PAR 7200 z dwoma kontrolerami o dodatkową półkę dyskową wraz z 16 dyskami 3,5" 2TB 6G NL-SAS 7.2K wraz z wymaganymi licencjami oraz niezbędnymi elementami montażowymi i elementami umożliwiającymi logiczne podłączenie do istniejącego środowiska. Gwarancja i rękojmia na dostarczone urządzenia - 36 miesięcy. W okresie gwarancji czas reakcji serwisu od momentu zgłoszenia usterki w ciągu jednego dnia roboczego. Dostarczona półka dyskowa, dyski oraz gwarancja muszą zostać fabrycznie zintegrowane ze sobą.

Sprzęt musi pochodzić z oficjalnego autoryzowanego kanału dystrybucyjnego zgodnego z siedzibą terytorialną Oferenta a oferta musi być potwierdzona oświadczeniem producenta sprzętu.

Sprzęt musi być fabrycznie nowy i wyprodukowany nie wcześniej niż 6 miesięcy przed dostawą. Zamawiający zastrzega sobie prawo weryfikacji pochodzenia sprzętu u Producenta i w przypadku zastrzeżeń, iż dostarczony sprzęt nie pochodzi z oficjalnego kanału dystrybucyjnego zgodnego z siedzibą terytorialną Oferenta oraz nie jest nowy, Zamawiający będzie domagał się wymiany sprzętu na właściwy a wszelkie koszty z tym związane ponosi Oferent.

4. Oprogramowanie do katalogowania zeskanowanych plików PDF

= praca w środowisku zgodnym z systemami Microsoft Windows od wersji 7 wzwyż,
= wykonane w technologii .NET i MS-SQL lub innej podobnej,
= aplikacja powinna być zintegrowana ze środowiskiem AD w celu pobierania uprawnień do jej obsługi,
= obsługa z klasycznego okienkowego interfejsu użytkownika. Nie dopuszcza się obsługi z okna przeglądarki internetowej,
= oprogramowanie ma katalogować pliki PDF na podstawie informacji z OCR, umieszczać w bazie danych i podpisywać certyfikatem z wskazanego CA,
= aplikacja powinna logować zdarzenia i transakcje w dowolnej lokalizacji,
= aplikacja powinna umożliwiać robienie kopii zapasowych konfiguracji i danych,
= wraz z oprogramowaniem mają być przekazane Zamawiającemu autorskie prawo majątkowe oraz kod źródłowy,
= wsparcie producenta i gwarancja 12 m-cy,
= czas reakcji serwisu na podjęcie naprawy gwarancyjnej w terminie 3 dni roboczych od daty zgłoszenia,

= przeszkolenie z obsługi w siedzibie zamawiającego.

5. Wdrożenia - według poniższej kolejności:

A. aktualizacja systemów klienckich sumarycznie 52 sztuk: Microsoft Windows 7 (x86 i x64) PRO PL OEM i Microsoft Windows 8,1 (x64) PRO PL OEM do Windows 10 PRO PL Aktualizacja musi zostać przeprowadzona fizycznie na każdym ze stanowisk przy zapewnieniu ciągłości pracy tj. maksymalnie 5 wyznaczonych komputerów dziennie. Aktualizacja w wersji finalnej musi posiadać zainstalowane wszystkie wymagane na dzień przekazania aktualizacje wymagane i zalecane przez producenta systemu operacyjnego.

B. migracja AD środowiska serwerowego z poziomu 2003 do 2012 (minimum dwa kontrolery).

C. wdrożenie środowiska Active Directory w ramach istniejącej infrastruktury na urządzeniach klienckich.

D. wdrożenie usługi WSUS i uruchomienie 52 jednostek komputerowych do korzystania z usługi WSUS.

E. wdrożenie centrum certyfikacji; Zaprojektowanie i wdrożenie infrastruktury klucza publicznego (PKI):

= zaprojektowanie infrastruktury CA zgodnie z przyjętymi dobrymi praktykami (co najmniej 2 urzędy CA),

= dostosowanie istniejącej usługi katalogowej (Active Directory) do ról CA,

= infrastruktura PKI powinna być przygotowana co najmniej do poniższych scenariuszy:

a) możliwość bezpiecznego wystawienia certyfikatu dla urządzeń sieciowych (zaimplementowana obsługa SCEP),

b) zabezpieczony ruch HTTPS,

c) szyfrowany system plików wspierany natywnie przez używany w MODGiK system operacyjny,

d) obsługa S/MIME,

= możliwość zastosowania i dostosowania szablonów certyfikatów pokrywających się co najmniej z ww. scenariuszami,

= możliwość zażądania wystawienia certyfikatu przez wewnętrzny portal WEB (HTTPS),

= możliwość dostarczenia certyfikatu dla urządzenia, usługi, użytkownika tylko tam gdzie jest to konieczne,

= możliwość dostarczenia certyfikatu za pomocą zasad grupy dla wybranych urządzeń,

= możliwość weryfikacji/walidacji certyfikatu z uwzględnieniem co najmniej następujących źródeł list CRL: LDAP, HTTP, FTP, OCSP,

= natywne wsparcie urzędu CA do odnowienia certyfikatu przy zachowaniu istniejącej pary kluczy (dla wybranych szablonów i scenariuszy),

= udokumentowane procedury tworzenia kopii zapasowej i odtworzenia z kopii bazy danych CA,

= możliwość przechowania w bazie CA kopii klucza prywatnego dla wybranych szablonów certyfikatów,

= zaprojektowanie, skonfigurowanie i wdrożenie infrastruktury PKI pod obsługę protokołu 802.1X.

F. wdrożenie systemu RADIUS; usługa powinna:

= wspierać co najmniej dwa mechanizmy uwierzytelniania użytkowników: lokalna baza użytkowników, usługa katalogowa LDAP (zgodna z używaną w MODGiK: Active Directory),

= natywną ochronę dostępu do sieci obsługiwaną przez używane w MODGiK systemy operacyjne (NAP) co najmniej w następujących scenariuszach wymuszeń (IPSEC, IEEE 802.1X),

= obsługiwać co najmniej następujących klientów RADIUS: bezprzewodowe punkty dostępowe, przełączniki 802.1X, serwery VPN,

= zapewnić centralną administrację z możliwością utworzenia i zarządzania szablonami konfiguracyjnymi dla poszczególnych typów klientów,

= zapewnić możliwość utworzenia bezpiecznych szablonów używanych haseł na potrzeby klientów RADIUS,

= zapewnić możliwość przechowywania zdarzeń RADIUS w centralnej bazie SQL dostępnej lokalnie lub na zdalnym komputerze,

= zapewnić możliwość utworzenia grupy serwerów RADIUS,

= zapewnić możliwość utworzenia polis zapewniających walidację i kontrolowanie przychodzących połączeń m.in. w zakresie akceptowanych: godzin i dni tygodnia, algorytmów i protokołów uwierzytelniania, grup użytkowników i urządzeń znajdujących się w usłudze katalogowej (Active Directory)

Wdrożeniem powinny zajmować się min. 2 różne osoby posiadające wykształcenie wyższe informatyczne, z certyfikatami MCSE Server Infrastructure, MCSE Desktop Infrastructure, Microsoft Specialist Server Virtualization.

6. Szkolenia administratorów

Omówienie zagadnień i szczegółowe zapoznanie z wiedzą teoretyczną administratorów w zakresie przeprowadzonych wdrożeń:

MICROSOFT WINDOWS 10:

A. Konfiguracja urządzeń z Windows 10

- Omówienie narzędzi programowych, których można użyć do konfigurowania Windows 10
- Opcje konfiguracyjne i zarządzanie kontami użytkowników

B. Zarządzanie magazynem danych

- Przegląd opcji przechowywania
- Zarządzanie dyskami, partycjami i wolumenami

C. Zarządzanie plikami i drukarkami

- Konfigurowanie i zarządzanie dostępem do plików
- Konfigurowanie i zarządzanie folderami udostępnionymi
- Zarządzanie drukarkami

D. Zarządzania bezpieczeństwem danych

- Zabezpieczanie danych z użyciem systemu szyfrowania plików EFS
- Wdrażanie i zarządzanie funkcją BitLocker

E. Zarządzanie bezpieczeństwem w systemie Windows 10

- Ograniczenia zagrożeń za pomocą ustawień zabezpieczeń
- Konfigurowanie UAC

F. Zarządzanie ustawieniami bezpieczeństwa połączeń sieciowych

- Zapora systemu Windows – funkcje i konfiguracja
- Reguły zabezpieczeń połączeń IPSec – konfiguracja
- Windows Defender

G. Rozwiązywanie problemów i odzyskiwania

- Zarządzanie urządzeniami i sterownikami
- Odzyskiwanie plików
- Odzyskiwanie Windows 10

H. Utrzymanie Windows 10

- Aktualizacja systemu Windows z wykorzystaniem WSUS
- Monitorowanie systemu Windows 10
- Optymalizacja wydajności
- Analiza i rozwiązywanie problemów dotyczących połączeń sieciowych IPv4, IPv6

- Analiza i rozwiązywanie problemów dotyczących dostępu do zasobów w obrębie domeny ADDS
- Analiza i rozwiązywanie problemów dotyczących dostępu do zasobów dla klientów niebędących członkami domeny

I. Wdrażanie systemu Windows 10

- Budowanie referencyjnego obrazu na WADK
- Korzystanie z MDT, aby wdrożyć system Windows 10
- Utrzymanie systemu Windows 10 Instalacja przy użyciu Windows ICD

J. Zarządzanie pulpitu i aplikacji. Ustawienia za pomocą zasad grupy

- Konfiguracja Group Policy Objects and Settings
- Analiza i rozwiązywanie problemów dotyczących zasad grupy GPO

ACTIVE DIRECTORY 2012:

A. Wprowadzenie do usług Active Directory

- Omówienie usług Active Directory i systemu DNS,

B. Struktury domeny

- Działanie domen
- Lasy domen i drzewa domen
- Działanie jednostek organizacyjnych
- Lokacje i podsieci

C. Praca z domenami usługi Active Directory

- Posługiwanie się komputerami za pomocą usługi Active Directory
- Poziomy funkcjonalne domeny
- Podwyższanie lub obniżanie poziomu funkcjonalnego lasu i domeny

D. Struktura katalogu

- Analiza magazynu danych
- Analiza wykazów globalnych
- Replikacja a usługa Active Directory
- Usługa Active Directory a protokół LDAP

E. Korzystanie z funkcji Active Directory Recycle Bin

F. Narzędzia zarządzania usługami Active Directory

G. Zarządzanie kontami komputera

- Tworzenie kont komputerów przy pomocy różnych narzędzi
- Przeglądanie i edytowanie właściwości konta komputera
- Usuwanie, wyłączanie i włączanie kont komputerów

- = Resetowanie zablokowanych kont komputerów
- = Przenoszenie kont komputerów
- = Zarządzanie komputerami
- = Przyłączanie komputera do domeny lub grupy roboczej
- = Stosowanie funkcji dołączenia domeny w trybie offline

H. Zarządzanie kontrolerami domen, rolami i katalogami

- = Instalowanie i obniżanie poziomu kontrolerów domen
- = Przeglądanie i transferowanie ról w całej domenie
- = Przeglądanie lub transferowanie roli wzorca nazw domeny
- = Przeglądanie i przenoszenie ról wzorców schematu
- = Przenoszenie ról przy użyciu wiersza poleceń
- = Przejmowanie ról przy użyciu wiersza poleceń
- = Konfigurowanie wykazów globalnych
- = Konfigurowanie buforowania członkostwa w grupach uniwersalnych

I. Zarządzanie jednostkami organizacyjnymi

- = Tworzenie jednostek organizacyjnych
- = Przeglądanie i edytowanie właściwości jednostki organizacyjnej
- = Zmiana nazwy lub usuwanie jednostki organizacyjnej
- = Przenoszenie jednostek organizacyjnych

J. Konserwacja usługi Active Directory

- = Stosowanie programu ADSI Edit

K. Rozwiązywanie problemów dotyczących usługi Active Directory

L. Różnice pomiędzy kontami użytkowników i grup

M. Domyślne konta użytkowników i grupy

- = Wbudowane konta użytkowników
- = Predefiniowane konta użytkowników
- = Wbudowane i predefiniowane grupy
- = Grupy niejawne i tożsamości specjalne

N. Możliwości konta

- = Uprawnienia
- = Prawa logowania
- = Wbudowane możliwości grup w usłudze Active Directory

O. Stosowanie kont grup domyślnych

- = Grupy używane przez administratorów

- = Grupy niejawne i tożsamości specjalne

P. Konfigurowanie i organizacja kont użytkowników

- = Zasady nazewnictwa kont
- = Zasady kont i haseł

Q. Konfigurowanie zasad kont

- = Konfigurowanie zasad haseł
- = Konfigurowanie zasad blokady konta

R. Konfigurowanie zasad praw użytkowników

- = Konfigurowanie globalnych praw użytkownika
- = Konfigurowanie lokalnych praw użytkownika

S. Dodawanie konta użytkownika

- = Tworzenie kont użytkowników domeny
- = Tworzenie kont użytkowników lokalnych

T. Dodawanie konta grupy

- = Tworzenie grupy globalnej
- = Tworzenie grupy lokalnej i przypisywanie członków

U. Obsługa członkostwa grup globalnych

- = Zarządzanie indywidualnym członkostwem
- = Zarządzanie wieloma członkostwami w grupie
- = Definiowanie grupy podstawowej dla użytkowników i komputerów

V. Implementowanie kont zarządzanych

- = Tworzenie i używanie zarządzanych kont usługi
- = Konfigurowanie usług, by stosowały zarządzane konta usług
- = Usuwanie zarządzanych kont usługi
- = Przenoszenie zarządzanych kont usługi
- = Stosowanie kont wirtualnych

W. Zarządzanie informacjami kontaktowymi użytkownika

- = Ustawianie informacji kontaktowych
- = Wyszukiwanie użytkowników i grup w usłudze Active Directory

X. Konfigurowanie ustawień środowiska użytkownika

- = Systemowe zmienne środowiskowe
- = Skrypty logowania
- = Przypisywanie katalogów macierzystych

Y. Ustawianie opcji i ograniczeń dla konta

- = Zarządzanie dozwolonymi godzinami logowania
- = Określanie, które stacje robocze są dopuszczane
- = Ustawianie uprawnień sieci VPN
- = Ustawianie opcji zabezpieczeń konta

Z. Zarządzanie profilami użytkowników

- = Profile lokalne, mobilne i obowiązkowe
- = Używanie narzędzia System do zarządzania profilami lokalnymi

AA. Aktualizowanie kont użytkowników i grup

- = Zmiana nazwy kont użytkowników i grup
- = Kopiowanie kont użytkowników domeny
- = Importowanie i eksportowanie kont
- = Usuwanie kont użytkowników i grup
- = Zmiana i resetowanie haseł
- = Włączanie kont użytkownika

BB. Zarządzanie wieloma kontami użytkowników

- = Ustawianie profilów dla wielu kont
- = Ustawianie godzin logowania dla wielu kont
- = Określanie dla wielu kont stacji roboczych, z których można się logować
- = Ustawianie logonu, hasła i daty ważności dla wielu kont

CC. Rozwiązywanie problemów dotyczących logowania

DD. Przeglądanie i ustawianie uprawnień usługi Active Directory

WSUS:

- Przygotowanie do wdrożenia usług WSUS (wybór scenariusza wdrażania usług WSUS, strategii przechowywania usług WSUS, zaprojektowanie usług WSUS pod kątem optymalizacji wydajności, przygotowanie planu konfiguracji ustawień aktualizacji automatycznych dla przyjętego scenariusza),
- Instalowanie roli serwera usług WSUS,
- Konfigurowanie usług WSUS (kreator konfiguracji programu WSUS, utworzenie grup komputerów w konsoli administracyjnej programu WSUS na użytek zarządzania aktualizacjami w organizacji, konfiguracja protokołu Secure Sockets Layer (SSL) do wspomagania ochrony programu WSUS),
- Zatwierdzanie i wdrażanie aktualizacji programu WSUS (tworzenie grup komputerów, konfigurowanie programu WSUS w celu automatycznego zatwierdzania instalacji

aktualizacji dla wybranych grup, przegląd zainstalowanych aktualizacji, komputerów, na których odebrano te aktualizacje, oraz innych szczegółów za pomocą funkcji Raportowanie programu WSUS),

- Konfiguracja ustawień zasad grupy dla funkcji aktualizacji automatycznych.

URZĄD CERTYFIKACJI I CERTYFIKATU SERWERA ZASAD SIECIOWYCH:

- Instalowanie roli serwera usług certyfikatów w usłudze Active Directory.
- Konfigurowanie szablonu certyfikatu serwera i automatycznego rejestrowania.
- Odświeżanie zasad grupy na serwerach zasad sieciowych.

RADIUS:

Serwer usługi RADIUS dla bezprzewodowych i przewodowych połączeń 802.1X

- Instalowanie i konfigurowanie serwerów dostępu do sieci (NAS) jako klientów usługi RADIUS,
- Wdrożenie składników dla metod uwierzytelniania,
- Konfigurowanie serwera NPS jako serwera usługi RADIUS,
- Omówienie obsługi uwierzytelniania w standardzie IEEE (Institute of Electrical and Electronics Engineers) 802.1X,
- Obsługa uwierzytelniania usługi RADIUS i ewidencjonowania aktywności usługi RADIUS,
- Funkcje filtrowania,
- Wdrażanie składników metod uwierzytelniania,
- Konfigurowanie serwera NPS jako serwera usługi RADIUS,
- Konfigurowanie zasad sieciowych,
- Konfigurowanie ewidencjonowania aktywności usługi RADIUS.

Całkowity czas trwania szkoleń - minimum 10 dni roboczych. Szkolenia przeprowadzone przez autoryzowanego trenera z uprawnieniami MCT w siedzibie zamawiającego, w godz. 8.00 - 15.00.