**SZCZEGÓŁOWY OPIS PRZEDMIOTU ZAMÓWIENIA**

**Rozbudowa infrastruktury macierzy obiektowych w środowisku Zamawiającego**

1. **Definicje**

**POPD** – Podstawowy Ośrodek Przetwarzania Danych.

**OOPD** – Odizolowany Ośrodek Przetwarzania Danych znajdujący się w lokalizacji jednostki organizacyjnej prokuratury.

**Oprogramowanie** – wartości niematerialne i prawne dostarczane w ramach przedmiotowego postępowania.

**ITS** – infrastruktura techniczno-systemowa.

**Urządzenie/Sprzęt** – sprzęt teleinformatyczny dostarczany w ramach przedmiotowego postępowania.

1. **Macierz obiektowa – 1 sztuka**

**Producent \* ………………………….….**

**Model, typ \* ……………………….…….**

| Identyfikator wymagania | Wymaganie | Opis wymagania |
| --- | --- | --- |
| MOBR-01 | Obiektowy system składowania danych | 1. Dostarczane rozwiązanie (obiektowy system składowania danych) musi być obecne na rynku od co najmniej 5 lat.
2. Dostarczane rozwiązanie musi być produktem rozpoznawalnym na rynku, co oznacza, że musi być wymieniane w raportach niezależnych organizacji, takich jak Gartner, IDC, Gigaom lub ESG (Enterprise Strategy Group).
3. Oferowane rozwiązanie musi być produktem gotowym, posiadającym na moment składania oferty wszystkie wymagane przez Zamawiającego funkcjonalności.
4. Oferowane urządzenia i wszystkie jego elementy składowe muszą pochodzić od autoryzowanego Dostawcy producenta, być fabrycznie nowe i wyprodukowane nie wcześniej niż pół roku przed terminem dostawy do Zamawiającego.
5. Wraz z rozwiązaniem musi być dostarczony komplet nośników umożliwiający odtworzenie oprogramowania systemowego urządzeń, z których zbudowane jest dostarczone rozwiązanie.
6. Dostarczona macierz ma działać jako odizolowany sieciowo (tzw. Airgap) tzw. bunkier cyfrowy dla posiadanych przez Zamawiającego danych obiektowych.
7. Wraz z rozwiązaniem musi zostać dostarczone wraz z narzędziem do ochrony przed złośliwym oprogramowaniem typu ransomware dla posiadanych przez zamawiającego macierzy Dell ECS (2 sztuki o łącznej pojemności 3,5PB).
8. Ochrona przed oprogramowaniem typu ransomware musi spełniać następujące wymagania:

-musi być rozwiązaniem obecnym na rynku od co najmniej 5lat;-musi umożliwiać instalację lokalną na platformie Linux w strefie bez dostępu do Internetu – preferowany system operacyjny Centos lub RedHat;-musi mieć możliwość zarządzania z interfejsu tekstowego za pośrednictwem SSH;-musi mieć możliwość zarządzania z interfejsu graficznego w postaci wbudowanej aplikacji lub za pośrednictwem przeglądarki www;-musi mieć możliwość przygotowania skryptów batch w postaci plików XML umożliwiających uruchomienie synchronizacji danych pomiędzy macierzami obiektowymi z zastosowaniem protokołu S3 w dowolnie wybranym czasie w oparciu o crontab;-musi mieć możliwość przesyłania danych do bucketów o innej nazwie niż buckety źródłowe;-musi dokonywać porównania zawartości bucketów po stronie źródłowej i docelowej w taki sposób aby kopiowane były jedynie nowe lub zmienione dane po stronie źródłowej;-musi umożliwiać pracę z autoryzacją w oparciu o różne dane autoryzacyjne i poziomy uprzywilejowania po stronie macierzy źródłowej i docelowej;-nie może wymagać do działania kont administracyjnych typu root, admin, administrator itp. po stronie macierzy źródłowej i docelowej;-musi mieć możliwość integracji z systemem antywirusowym; |
| MOBR-02 | Dostęp i protokoły | 1. Rozwiązanie musi posiadać możliwość dostępu do danych co najmniej za pomocą następujących interfejsów i protokołów: Amazon S3, OpenStack Swift oraz NFS. Jeżeli wykorzystanie któregokolwiek z wymienionych protokołów wymaga zastosowania dodatkowej licencji lub oprogramowania, to należy je dostarczyć wraz z rozwiązaniem.
2. System musi umożliwiać jednoczesny dostęp do tych samych danych przy pomocy wszystkich wymaganych protokołów (Amazon S3, OpenStack Swift, NFS).
3. Rozwiązanie dodatkowo musi posiadać możliwość natywnego (t.j. bez pośrednictwa serwerów) dostępu do danych za pomocą protokołów Centera CAS oraz Atmos.
4. Dane w obiektowym systemie składowania danych będącym przedmiotem zapytania muszą być składowane jako obiekty składające się z danych oraz opisujących je metadanych. Metadane nie mogą być składowane w wydzielonej bazie danych, a replikacja danych (obiektów) obywa się spójnie z metadanymi.
5. Dla protokołu S3 rozwiązanie musi posiadać wbudowany mechanizm indeksowania i przeszukiwania metadanych. Musi istnieć możliwość wyszukiwania w oparciu o wewnętrzną wyszukiwarkę lub interfejs API pozwalający na integrację silnika wyszukiwania z własną aplikacją.
6. Rozwiązanie musi posiadać możliwość zdefiniowania kluczy metadanych do indeksowania.
7. Per Bucket musi istnieć możliwość zdefiniowania min. 30 kluczy do indeksowania.
8. Rozwiązanie musi posiadać wbudowany mechanizm wersjonowania obiektów w przypadku wykorzystania protokołu S3.
9. Platforma musi umożliwiać zarządzanie listami kontroli dostępu ACL oraz politykami dostępu do Bucket'ów (Bucket Policy), przy pomocy których można definiować uprawnienia przyznawane użytkownikom.
10. Urządzenie musi wspierać autentykację przy pomocy mechanizmu IAM (Identity and Access Management).
 |
| MOBR-03 | Sprzęt | 1. Platforma musi być zbudowana w architekturze scale-out (skalowalnej horyzontalnie).
2. Oferowana macierz musi być zarządzana z posiadanego interfejsu zarządzania infrastrukturą macierzy obiektowych ECS oraz umożliwiać połączenie i uruchomienie natywnej (tzn. bez pośrednictwa serwerów) replikacji z posiadanymi przez Zamawiającego macierzami obiektowymi Dell ECS.
3. Dostarczony sprzęt musi posiadać pojemność przynajmniej 1,7PB brutto.
4. Rozwiązanie musi umożliwiać skalowanie poprzez dokładanie kolejnych kontrolerów i/lub dysków. Wymagana jest skalowalność do pojemności min 100PB. Rozbudowa rozwiązania musi być bezprzerwowa.
5. Dostarczany system musi umożliwiać zapisanie co najmniej 10 mld obiektów bez konieczności rozbudowy czy dodawania węzłów.
6. Wymagana pojemność musi być dostarczona na dyskach twardych znajdujących się wewnątrz węzłów rozwiązania. Nie są dopuszczalne rozwiązania oparte o taśmy lub platformy chmurowe.
7. Dopuszczalne są dyski typu SATA lub NL-SAS nie większe niż 12TB.
8. Dane muszą być chronione przy pomocy kodowania nadmiarowych (Erasure Coding) na wewnętrznych dyskach kontrolerów. Rozwiązanie nie dopuszcza stosowania struktur typu RAID czy LUN wymagających dodatkowego administrowania.
9. Przestrzeń służąca do przechowywania danych musi być skonfigurowana tak, aby była odporna na jednoczesną awarię co najmniej 2 dowolnych dysków twardych lub kontrolerów (tzn. taka awaria nie musi prowadzić do utraty danych).
10. Dostęp do rozwiązania musi być realizowany za pomocą protokołu Ethernet oraz interfejsów 10Gb lub 25Gb.
11. W przypadku, gdy system wymaga przełączników na potrzeby wewnętrznej i/lub zewnętrznej komunikacji, należy zapewnić redundantne przełączniki LAN 10Gb lub 25Gb z odpowiednią liczbą portów.
12. Urządzenie nie może posiadać pojedynczego punktu awarii, tzn. wszystkie jego elementy muszą być redundantne, a jego architektura musi zapewniać odporność na awarię w obrębie poszczególnych grup elementów, przynajmniej w zakresie dysków, interfejsów dostępowych, kontrolerów, zasilaczy i wentylatorów.
13. Rozwiązanie musi mieć możliwość podłączenia go do centrum serwisowego producenta w celu zdalnego monitorowania poprawności funkcjonowania komponentów rozwiązania.
14. Ze względu na wysoką dostępność, oferowane urządzenie musi umożliwiać dostęp do danych bezpośrednio przez wszystkie dostarczone kontrolery (t.j. bez wydzielonych kontrolerów dostępowych, management'owych, storage'owych itd)
15. Oferowane rozwiązanie musi być oparte o kontrolery o wysokości nie większej niż 2RU
16. Ze względu na wydajność i dostępność wszystkie kontrolery dostarczanego rozwiązania muszą umożliwiać dostęp do danych (tzn. nie musi być węzłów dedykowanych oddzielnych węzłów dostępowych).
17. Oferowane rozwiązanie musi być dostarczone w jednej dedykowanej przez producenta rozwiązania szafie stelażowej (Rack) o wysokości co najmniej 40U wyposażonej w co najmniej dwie listwy zasilające (PDU) umożliwiające podłączenie do dwóch różnych obwodów zasilających i zakończonych wtykami jednofazowymi 32A. PDU oraz konstrukcja szafy musza umożliwiać instalacje w niej co najmniej 16 kontrolerów.
 |
| MOBR-04 | Replikacja | 1. Urządzenie musi umożliwiać replikację w technologii geograficznie rozproszonego klastra pracującego w trybie active/active, tzn. te same dane (obiekty) muszą być dostępne w trybie odczyt/zapis w obu ośrodkach jednocześnie.
2. W replikacji active/active system musi mieć możliwość pracy w trybie tzw. "strong consistency" tzn. musi zwracać najbardziej aktualną wersję obiektu, niezależnie od tego, do którego ośrodka trafi zapytanie.
3. Replikacja musi odbywać się w ramach szyfrowanego kanału. Funkcjonalność szyfrowania musi być wspierana przez platformę obektową.
 |
| MOBR-05 | Worm | 1. Przynajmniej dla protokołów Centera CAS oraz S3 system musi zapewniać i gwarantować niezmienność składowanych w nim obiektów poprzez wykorzystanie wbudowanej funkcjonalności WORM (Write Once Read Many). Funkcjonalność WORM musi być realizowana wewnątrz dostarczonego gotowego rozwiązania sprzętowego w jego oprogramowaniu systemowym.
2. Rozwiązanie musi posiadać możliwość definiowania różnych poziomów retencji przechowywania danych, gwarantujących brak możliwości skasowania danych przed upływem zdefiniowanego czasu.
3. Rozwiązanie musi pozwalać na zdefiniowanie partycji, w których istnieje możliwość usuwania danych przed upływem retencji oraz partycji (tzw. tryb Enterprise), w których usuwanie danych przed upływem retencji jest niemożliwe - również przez operatora/administratora platformy (tzw. tryb Compliance). Rozwiązanie musi pozwalać na definiowanie i uruchamianie jednocześnie obydwu typów partycji. Jeżeli ta funkcjonalność wymaga dodatkowej licencji, należy ją dostarczyć.
4. Rozwiązanie natywnie (tzn. bez hostów pośredniczących) musi wspierać replikację do innych targetów S3 (np. bucket S3 w Amazon AWS)
5. Wymagana wsparcie dla S3 ObjectLock.
6. Dla funkcjonalności WORM urządzenie musi spełniać wymagania standardu SEC 17-a4 oraz FIPS.
 |
| MOBR-06 | Multi-tennancy | 1. Rozwiązanie musi posiadać możliwość tworzenie logicznie odseparowanych obszarów tzw. „MULTI-TENANCY”. Wymagana jest możliwość rozdzielnego administrowania (np.: przypisywanie użytkowników, tworzenie praw dostępu, polityki składowania danych, monitorowanie wykorzystania) tak tworzonymi obszarami.
2. Zamawiający wymaga, aby dostarczone rozwiązanie posiadało możliwość zdefiniowania co najmniej 1000 logicznych partycji ("tennant'ów").
3. Musi istnieć możliwość mapowania zasobów do różnych zastosowań w taki sposób, aby dla każdego z nich możliwe było definiowanie różnych i niezależnych parametrów i kryteriów składowania danych w tym, co najmniej: retencji, quoty, indeksowania i replikacji.
 |
| MOBR-07 | Inne | 1. Wymagana jest możliwość autentykacji z użyciem AD/LDAP.
2. Rozwiązanie musi posiadać swoje własne wbudowane mechanizmy weryfikacji integralności danych np przy pomocy sum kontrolnych składowanych obiektów.
3. Rozwiązanie musi posiadać wbudowane mechanizmy redukcji danych, w tym co najmniej kompresję danych. W przypadku braku tej funkcjonalności, należy dostarczyć 100% więcej pojemności.
4. Rozwiązanie musi posiadać funkcjonalność szyfrowania danych przechowywanych na dyskach obiektowego magazynu składowania danych. Wymagane jest użycie alrytmu min. AES-256 lub równoważnego. Jeżeli wymagana jest licencja, należy ją dostarczyć.
5. Wymagane jest wsparcie dla komend API S3 Select.
 |
| MOBR-08 | Zarządzanie i monitrowanie | 1. Rozwiązanie musi umożliwiać:
2. - Zarządzanie co najmniej poprzez graficzny interfejs użytkownika oraz poprzez API.
3. - Automatyczny monitoring obejmujący m.in.: utylizację zasobów on-line (w tym CPU, pamięć, sieć), zajętość miejsca, tranfery, czy ilość operacji.
4. - Tworzenie alertów i powiadomień dot. stanu SYSTEMU, automatyczne przesyłanie ich poprzez e-mail."
 |
| MOBR-09 | Dodatkowe | 1. Rozwiązanie musi wspierać APLIKACJE BACKUPOWE (bezpośrednio bądź poprzez dodatkowy moduł konwersji zapisu „na dysk” na zapis „do chmury” – w tym wypadku SYSTEMU) jako medium „S3” do długoterminowego składowania danych, wsparcie musi być zapewnione dla wiodących aplikacji backup’owych pochodzących od producentów (min. 3-ech) określonych jako LEADERS w „Magic Quadrant for Data Center Backup and Recovery Solutions 2017”.
2. Wraz z rozwiązaniem należy dostarczyć komplet usług obejmujących instalację oraz wdrożenie zarówno macierzy, jak i oprogramowania.
 |
| MOBR-10 | Certyfikaty | 1. Certyfikat ISO 9001 dla producenta sprzętu obejmujący proces projektowania i produkcji – dołączony do oferty dokument potwierdzający spełnienie tego wymogu.
2. Certyfikat ISO 14001 dla producenta sprzętu – dołączony do oferty dokument potwierdzający spełnienie tego wymogu.
3. Urządzenia wyprodukowane są przez producenta, zgodnie z normą PN-EN ISO 50001 lub oświadczenie producenta o stosowaniu w fabrykach polityki zarządzania energią, która jest zgodna z obowiązującymi przepisami na terenie Unii Europejskiej – dołączony do oferty dokument potwierdzający spełnienie tego wymogu.
4. Deklaracja zgodności CE – dołączona do oferty.
5. Potwierdzenie spełnienia kryteriów środowiskowych, w tym zgodności z dyrektywą RoHS Unii Europejskiej o eliminacji substancji niebezpiecznych w postaci oświadczenia producenta serwera (wg wytycznych Krajowej Agencji Poszanowania Energii S.A, zawartych w dokumencie „Opracowanie propozycji kryteriów środowiskowych dla produktów zużywających energię możliwych do wykorzystania przy formułowaniu specyfikacji na potrzeby zamówień publicznych”, pkt 3.4.2.1; dokument z grudnia 2006 r.), w szczególności zgodności z normą ISO 1043-4 dla płyty głównej oraz elementów wykonanych z tworzyw sztucznych o masie powyżej 25 gr – dołączony do oferty dokument potwierdzający spełnienie tego wymogu.
6. Oświadczenie producenta macierzy, potwierdzające, że sprzęt pochodzi z oficjalnego kanału dystrybucyjnego producenta – dołączone do oferty.
 |
| MOBR-11 | Warunki gwarancji | 1. Gwarancja producenta 36 miesięcy, świadczona na miejscu u klienta.
2. Czas reakcji serwisu - do końca następnego dnia roboczego od chwili zgłoszenia.
3. Serwis urządzeń musi być realizowany przez producenta lub Autoryzowanego Partnera Serwisowego producenta – dołączone do oferty oświadczenie producenta potwierdzające, że serwis będzie realizowany przez Autoryzowanego Partnera Serwisowego producenta lub bezpośrednio przez producenta.
4. Firma serwisująca musi posiadać ISO 9001 na świadczenie usług serwisowych oraz posiadać autoryzację producenta serwera – dołączony do oferty dokument potwierdzający spełnienie tego wymogu.
5. W przypadku awarii dysku twardego, dysk pozostaje u Zamawiającego.
 |

1. **Zakres prac Wykonawcy**

|  |  |  |
| --- | --- | --- |
| Identyfikator wymagania | Wymaganie | Opis wymagania |
| PRAC-1 | Zakres usług Wykonawcy | 1. Wykonanie w uzgodnieniu z Zamawiającym Projektu technicznego zawierającego co najmniej:
	1. Rozmieszczenie sprzętu w szafie rack.
	2. Projekt zasilania energetycznego.
	3. Projekt połączeń do sieci LAN wdrażanego rozwiązania
	4. Wymagania dotyczące zasilania i klimatyzacji oraz wagi poszczególnych szaf rack,
	5. Projekt replikacji danych pomiędzy dostarczaną macierzą oraz posiadanymi przez Zamawiającego macierzami.
	6. Projekt monitorowania stanu macierzy.
	7. Konfiguracja przekazywania zdarzeń do rozwiązania SIEM posiadanego przez Zamawiającego oraz konfiguracja scenariuszy powodujących incydent bezpieczeństwa.
2. Wykonanie dokumentacji administracyjnej dla dostarczanych urządzeń i narzędzia do ochrony przed złośliwym oprogramowaniem typu ransomware. Dokumentacja administratora musi zawierać co najmniej:
	1. Procedury administracyjne;
	2. Procedury instalacji i konfiguracji;
	3. Procedury bieżących działań administracyjnych;
	4. Procedury okresowych/planowanych działań administracyjnych;
	5. Procedury aktualizacji oprogramowania narzędzia do ochrony przed złośliwym oprogramowaniem typu ransomware;
	6. Procedury włączenia i wyłączenia całości dostarczanego sprzętu i oprogramowania w przypadku prac planowych;
	7. Procedury awaryjne dla administratorów;
	8. Procedury kwalifikacji zgłoszeń serwisowych;
	9. Procedury eskalacji zgłoszeń serwisowych;
	10. Opis innych czynności/zadań, które wdrożył Wykonawca;
3. Wykonawca opracuje szczegółowe procedury eksploatacyjne wdrożonych komponentów warstwy fizycznej. Jako procedurę eksploatacyjną rozumie się opis zbioru czynności eksploatacyjnych mających na celu zrealizowane określonego zadania eksploatacyjnego np. wykonanie aktualizacji oprogramowania. Procedury muszą obejmować wszystkie czynności, jakie należy wykonać w celu monitorowania i utrzymania dostarczonych komponentów w poprawnym działaniu i zgodności z najnowszymi wersjami komponentów.
4. Dostawa kompletu Sprzętu, montaż, instalacja i konfiguracja w lokalizacji Prokuratury Krajowej lub w lokalizacji OOPD.
5. Montaż sprzętu według projektu w szafach rack.
6. Podłączenie do zasilania elektrycznego w lokalizacji Zamawiającego. Wykonawca dokona niezbędnych podłączeń elektrycznych w celu instalacji i zasilenia modułów PDU w szafie/ach rack w których zamontowane będą dostarczane urządzenia z dwóch torów zasilania w serwerowni Zamawiającego lub w lokalizacji zdalnej w celu podłączenia do zasilania elektrycznego. Przyłącza elektryczne będą prowadzone od rozdzielni elektrycznych w budynku (pomieszczeniu serwerowni) do paneli PDU w szafach rack. Każde urządzenie posiadające redundantne zasilacze zostanie podłączone do dwóch niezależnych torów zasilania elektrycznego. W każdej szafie rack pozostanie wolnych co najmniej 5 gniazd elektrycznych z każdego toru zasilania.
7. Aktualizacja oprogramowania wewnętrznego (firmware) elementów Sprzętu do najnowszych rekomendowanych wersji.
8. Podłączenie Sprzętu do sieci LAN wraz z konfiguracją (niezbędne okablowanie dostarcza Wykonawca).
9. Uruchomienie monitorowania macierzy zgodnie z wymaganiami Zamawiającego.
10. Przeprowadzenie testów działania skonfigurowanej macierzy oraz narzędzia do ochrony przed złośliwym oprogramowaniem typu ransomware. Wykonawca opracuje scenariusze testowe umożliwiające weryfikację spełnienia wymagań, poprawność instalacji i konfiguracji wszystkich komponentów. Wykonawca przeprowadzi testy sprawdzające niezawodność na wypadek awarii pojedynczego punktu infrastruktury według scenariuszy przygotowanych przez Wykonawcę i zatwierdzonych przez Zamawiającego.
11. Opracowanie dokumentacji powykonawczej.
12. Wykonawca dokona przeglądu i aktualizacji szacowania ryzyka dla systemów teleinformatycznych Zamawiającego korzystających z macierzy obiektowej uwzględniając rozwiązanie ochrony przed złośliwym oprogramowaniem typu ransomware dla macierzy obiektowych wdrożone w ramach projektu.
13. Wykonawca zaktualizuje Politykę Wykonywania Kopii Zapasowych oraz Politykę Ciągłości Działania Systemów Teleinformatycznych uwzględniając wdrożone rozwiązanie ochrony przed złośliwym oprogramowaniem typu ransomware dla macierzy obiektowych.
14. Wykonawca przeszkoli pracowników Zamawiającego z zakresu dostarczonej macierzy obiektowej oraz narzędzia do ochrony przed złośliwym oprogramowaniem typu ransomware zgodnie z poniższymi zasadami:
	1. Szkolenia zostaną przeprowadzone oddzielnie dla dwóch dwuosobowych grup administratorów i składać się będą z części merytorycznej i praktycznej. Każde Szkolenie trwać będzie nie mniej niż 8 godzin roboczych.
	2. Koszty związane z organizacją szkolenia i przebiegiem szkolenia, w tym koszt materiałów edukacyjnych, wynajęcia sali, sprzętu i innych elementów składających się na całą usługę szkoleniową pokrywa Wykonawca.
	3. Termin przeprowadzenia szkoleń zostanie ustalony po podpisaniu umowy.
	4. Szkolenie będzie prowadzone poza siedzibą Zamawiającego dla grupy 5-osobowej, tj. w autoryzowanym ośrodku szkoleniowym producenta sprzętu lub partnera uprawnionego do przeprowadzenia szkoleń w Warszawie.
	5. Szkolenie musi być przeprowadzone przez osoby posiadające certyfikaty potwierdzające kompetencje do prowadzenia szkoleń z zakresu danego rodzaju Sprzętu.
	6. Merytoryczna zawartość szkolenia musi zawierać:
		1. Szkolenie musi zapoznać uczestników z architekturą, administracją i konfiguracją.
		2. Szkolenie musi zapoznać uczestników z oprogramowaniem do zarządzania.
		3. Szkolenie musi zapewnić ćwiczenia praktyczne.
		4. Szkolenie musi zapoznać uczestników ze zmianami wprowadzonymi w Polityce Wykonywania Kopii Zapasowych oraz Polityce Ciągłości Działania Systemów Teleinformatycznych
	7. Szkolenia będą prowadzone w języku polskim.
15. Wykonawca przeprowadzi warsztaty z zakresu każdego z typów urządzeń dostarczanych w ramach przedmiotowego postępowania. Warsztaty muszą trwać przynajmniej 1 dzień roboczy i uwzględniać uwarunkowania montażu i instalacji sprzętu w infrastrukturze Zamawiającego.
16. Warsztaty odbędą się w siedzibie Zamawiającego. Warsztaty będą prowadzone w języku polskim. Osoba/osoby prowadzące będą posiadać odpowiednią wiedzę, przygotowanie merytoryczne umożliwiające przekazanie informacji z zakresu wdrożonych rozwiązań.
17. Wykonawca zobowiązany będzie do przygotowania i przedstawienia Zamawiającemu, co najmniej na 10 dni przed rozpoczęciem szkoleń oraz warsztatów, odpowiednich materiałów szkoleniowych, włączając w to materiały dla uczestników. Zamawiający zastrzega prawo do żądania wprowadzenia poprawek i zmian do materiałów szkoleniowych.
 |

UWAGI ZAMAWIAJĄCEGO:

(\*) W ofercie należy podać nazwę producenta, typ oraz model oferowanego sprzętu umożliwiający jednoznaczną identyfikację oferowanej konfiguracji.