**Załącznik nr 3 do SWZ**

**SZCZEGÓŁOWY OPIS PRZEDMIOTU ZAMÓWIENIA**

**Zakup wyposażenia serwerowni Urzędu Gminy Trąbki Wielkie w ramach projektu grantowego „Cyfrowa Gmina”.**

1. **Szafa rack – zestaw – 1 szt.**

|  |  |
| --- | --- |
| **Nazwa komponentu** | **Wymagane minimalne parametry techniczne** |
| Standard RACK | 19' |
| Typ | Stojąca serwerowa |
| Marka | SIGNAL |
| Zastosowanie | wewnętrzne |
| Wymiary (wys./gł./szer.) | 32U, 1600x800x600 mm; |
| Zgodność z normami | PN-EN 62368-1:2015-03 |
| Materiał | Stal |
| Nośność | 800 kg. |
| Drzwi przednie | Perforowane |
| Drzwi tylne | Preforowna, dwuskrzydłowe, możliwość montażu lewo/prawo; |
| Ściany boczne | Zdejmowame, wyposażone w zamek i 12 kluczyków; |
| Szyny montażowe | 4 szt. z oznaczeniami jednostki U w postaci znaczników i numerów; |
| Organizer przewodów | 2 szt. |
| Klamka | Z zamkniem; |
| Otwory na przewody | W suficie i podłodze; |
| Otwory wentylacyjne | W tylnej ścianie, suficie, podłodze, drzwiach; |
| Otwory na wentylatory | 4 szt., 100x100 mm |
| Zgodność z normami | PN-EN 62368-1:2015-03, PN-EN ISO/IEC 17067:2014-01 – **załączyć do oferty certyfikat potwierdzający, wystawiony przez niezależny podmiot certyfikacyjny;** |
| Wymagania dodatkowe | Złącze uziemiające, możliwość montażu kółek i nóżek, kólka i nóżki w zestawie z szafą, możliwość montażu cokołu |
| Listwa zasilająca | 2 listwy mocowane do szyn o wysokości maksymalnie 1U każda i głębokości maksymalnie 60 mm każda.9 złącz NFC61-314;Przewód zasilający o długości 160 cm.;Przycisk załączenia i dioda LED;Napięcie – 250 VAC;Prąd – 16 A; |
| Patch panel | 6 x patch panel z 24 slotami na moduł keystone każdy;Mocowane doczołowo do szyn rack;Wysokośc 1U, głębokość maksymalnie 130 mm.Materiał – stal;Uchwyt na przewody; |
| Moduły keystone | 144 x RJ45, kat. 6 UTP, beznarzędziowe;Muszą być przeznaczone do budowy nieekranowanych gniazd abonenckich oraz punktów krosowych w instalacjach zgodnych z kat.6.Złącza szczelinowe muszą posiadać kolorowe kodowanie ułatwiające prawidłową instalację w sekwencjach 568A lub 568B;* Złącza - IDC110/ Krone, 8P8C;
* Rodzaj połączenia – zaciskane;
* Montaż do obudowy;
* Kontakty z fosforobrązu platerowanego złotem

Zgodność z normami: EIA/TIA 586A, ISO 11801:2011, PN-EN 50173-1:2013 ROHS 2002/95/WE IEC 60603-7-1:2011 C – **załączyć do oferty potwierdzającą deklarację CE;** |
| Panel wentylatorów | Musi posiadać 3 wentylatory;Montowany doczołowo do szyn rack,;Wysokość 1U, głębokość maksymalnie 350 mm;Wbudowany włącznik;Zgodność z dyrektywą 89/336/EEC oraz normami: EN 55022:1988/A1:2000/A2:2003 Class B;EN 61000-3-2:2000/A1:2001, EN 61000-3-3:1995/A1:2001 EN 55024:1998/A1:2001/A2:2003 (IEC 61000 -4-2:1995/A2:2000, IEC 61000-4-3:2002, IEC 61000-4-4:1995/A2:2001, IEC 61000-4- 5:1995/A1:2000, IEC 61000-4-6:1996/A1:2000, IEC 61000-4- 9:1993/A1:2000, IEC 61000-4-11:1994/A1:2000 - – **załączyć do oferty potwierdzającą deklarację CE;** |
| Półki | 2 półki o wysokości maksymalnie 20 i głębokości 800 mm. każda;Mocowana 4-punktowo, w zestawie śrubki i koszyczki;Matriał – stalNosność każdej – 60 kg. |

1. **Przełącznik sieciowy – 3 szt.**

|  |  |
| --- | --- |
| **Nazwa komponentu** | **Wymagane minimalne parametry techniczne**  |
| Standardy i protokoły | IEEE 802.3i, IEEE 802.3u, IEEE 802.3ab, IEEE802.3z,IEEE 802.3ad, IEEE 802.3x, IEEE 802.1d, IEEE 802.1s,IEEE 802.1w, IEEE 802.1q, IEEE 802.1x, IEEE 802.1p, IEEE 802.3az |
| Porty | 48 portów RJ45 10/100/1000Mb/sAutomatyczna negocjacja szybkości połączeń i automatyczne krosowanie4 porty SFP 1000Mb/s1 port konsoli RJ451 port konsoli Micro-USB |
| Pobór mocy | Maksymalnie: 35W |
| Obudowa | rack |
| Przepustowość | 100 Gb/s |
| Szybkość przekierowań pakietów | 75Mp/s |
| Tablica adresów MAC | 16k |
| Bufor pakietów | 1,5 MB |
| Ramki jumbo | 9216 Bajtów |
| Quality of Service | Priorytetowanie ruchu w oparciu o standard IEEE 802.1p8 kolejekUstalenie kolejki priorytetów;Limitowanie transmisji w zależności od portu, przepływu danychVoice VLAN |
| Funkcje L2 i L2+ | Routing statycznyDHCP RelayIGMP Snooping V1/V2/V3Obsługa protokołu LACP zgodnie ze standardem 802.3ad (10 grup agregacji, 8 portów na grupę)Spanning Tree STP/RSTP/MSTPFiltrowanie/ochrona BPDUTC/Root ProtectWykrywanie pętli zwrotnychKontrola przepływu danych (802.3x)L2TP |
| Sieci VLAN | Wsparcie standardu IEEE802.1Q, 4096 VLAN i identyfikatorów VLANPort/MAC/Protocol/Private VLANGARP/GVRP |
| Listy kontroli dostępu | Filtrowanie pakietów oparte o źródłowe i docelowe adresy MAC;Adres IP, porty TCP/UDP, 802.1p, DSCP, VLAN IDdostęp ograniczony czasowo; |
| Bezpieczeństwo transmisji | Wiązanie IP-MAC-Port-VIDUwierzytelnianie oparte o standard IEEE 802.1X, RadiusOchrona przed atakami DoSDynamiczna ochrona przed atakami ARP)SSH v1/v2SSL v2/v3/TLSv1Zabezpieczenia portówBroadcast/Multicast/Unknown-unicast Storm Control |
| IPv6 | Podwójny stos IPv4/IPv6MLD SnoopingIPv6 NDWykrywanie MTUICMPv6TCPv6/UDPv6 |
| Zastosowania IPv6 | Klient DHCP, Ping, Tracert, Telnet, IPv6 SNMP, IPv6 SSH, IPv6 SSLHttp/Https, IPv6 TFTP, Interfejs IPv6, Routing IPv6, Przekaźnik DHCPv6, DHCPv6 Snooping |
| Zarządzanie | Interfejs przeglądarki internetowej GUI, interfejs linii poleceń CLISNMP v1/v2c/v3, zgodne z publicznymi i prywatnymi bibliotekami, RMON, klient DHCP/BOOTP, DHCP Snooping, DHCP Option82, Monitorowanie CPU, Port Mirroring, Synchronizacja czasu SNTP, aktualizacja firmwaru, diagnostyka, logi systemu, publiczne biblioteki; |
| Wymagania dodatkowe | Brak wentylatorów, zabezpieczenie fizyczne, zestaw do montażu w szafie rack; |

1. **Oprogramowanie specjalistyczne – 1 szt.**

# Musi umożliwiać  backup danych przez sieć komputerową z 30 komputerów i 2 serwerów fizycznych posiadanych przez zamawiającego;

1. Licencja musi być bezterminowa;
2. Bezpłatne [aktualizacje](https://www.ferrobackup.com/pl/faq.html#q3) w ramach tej samej wersji;
3. Licencje nie mogą być są przypisane do konkretnego komputera. Po odinstalowaniu z jednego komputera musi być mozliwośc instalacji na innym komputerze;
4. Program musi potrafić wykonać kopię tych części pliku (bloków), które uległy zmianie.
5. Dane muszą być kompresowane już po stronie komputera źródłowego;
6. Możliwość backupu całych dysków/partycji wraz z systemem operacyjnym i programami.
7. Backup musi być wykonywalny w czasie normalnej pracy komputera, zarówno w trybie pełnym jak i różnicowym;
8. Możliwość uruchomienia uszkodzonego komputera z płyty lub napędu USB i odzyskanie systemu operacyjnego wraz z zainstalowanym oprogramowaniem na nowym, czystym dysku twardym (bare metal recovery);
9. Mozliwośc wskazania które pliki lub katalogi mają być archiwizowane;
10. Mozliwośc uzywania symboli wieloznacznych (masek), aby wskazać nazwy lub rozszerzenia plików do archiwizacji i do wykluczenia z archiwizacji;
11. Możliwość archiwizacji i przywracania zaawansowanych właściwości systemu plików NTFS, takich jak: deskryptory zabezpieczenia ACL, właścicieli plików, atrybuty, dowiązania symboliczne i stałe, pliki zaszyfrowane EFS, BitLocker;
12. Backup plików, które są używane i zablokowane przez inne procesy;
13. Możliwość "cofnięcia się w czasie" i przywrócenia wybranego pliku lub całego dysku na stan z określonego dnia w przeszłości.
14. Możliwość cofnięcia zmian w uszkodzonych plikach, które powstały ze względu na działanie programów szyfrujących typu ransomware, locker, crypter, błąd ludzki lub awarię sprzętową;
15. Mozliwość automatycznego uruchomienia backupu kiedy użytkownik wyłącza komputer;
16. Mozliwość automatycznego uruchomienia archiwizacji zaraz po podłączeniu komputera do sieci firmowej;
17. Mozliwośc archiwizacji maszyn wirtualnych pracujących pod kontrolą [Microsoft Hyper-V](https://www.ferrobackup.com/pl/backup-odzyskiwanie-hyper-v.html) lub [VMWare ESX(i)](https://www.ferrobackup.com/pl/backup-maszyn-wirtualnych-esx.html);
18. Program musi działać w architekturze klient-serwer;
19. Możliwość równoległego wykonywania backupu z kilku komputerów; kompresji i szyfrowania po stronie stacji roboczej, backupu systemu operacyjnego;
20. Centralne sterowanie backupem komputerów z konsoli sterowania;
21. W konsoli musza być [widoczne są wszystkie komputery, ich dyski i pliki](https://www.ferrobackup.com/pl/screenshots.html);
22. Odzyskiwanie danych z serwera backupu.
23. Archiwizacja wykonywana w tle;
24. Możliwość zmiany priorytetu archiwizacji oraz ustalenia przedziału czasowy, w którym backup powinien być wykonywany wolniej, dla każdego komputera;
25. Wszystkie kopie musza być wyświetlane, jak kopie pełne;
26. Możliwość szyfrowania archiwów za pomocą [algorytmów z kluczem 256 bit](https://www.ferrobackup.com/pl/config.html#szyfrowanie-metoda) zapewniających bezpieczeństwo sieci i informacji wymaganych przez RODO;
27. Wbudowane technologie BitLocker i Encrypting File System (EFS).
28. Za każdym razem wykonywany musi być backup wszystkich wybranych dysków, katalogów lub plików.
29. Archiwizacja różnicowa na poziomie fragmentów plików;.
30. Backup baz danych i plików poczty
31. Możliwość wykonania backupu bazy danych bez zatrzymywania serwera bazodanowego oraz backupu dużych [plików pocztowych (Outlook \*.PST)](https://www.ferrobackup.com/pl/outlook-pst-backup.html) podczas godzin pracy;
32. Szyfrowanie archiwów i transferu za pomocą algorytmów Rijndael(AES), Serpent, Twofish.
33. Szyfrowanie po stronie stacji roboczej;
34. Dane musza być zabezpieczone już podczas przesyłu do serwera archiwizacji.
35. Archiwizacja i kompresja danych po stronie stacji roboczych;
36. Możliwość automatycznego duplikowania archiwów z serwera archiwizacji do innej lokalizacji sieciowej, na dodatkowy dysk twardy, [serwer NAS](https://www.ferrobackup.com/pl/backup-na-dysk-sieciowy.html), serwer FTP, napęd optyczny (CD/DVD/Blu-Ray/HD-DVD), [napęd taśmowy](https://www.ferrobackup.com/pl/archiwizacja-danych-na-naped-tasmowy.html) (DDS, DLT, LTO lub na [dysk w chmurze;](https://www.ferrobackup.com/pl/archiwizacja-w-chmurze-backup-online.html)
37. Oprogramowanie musi być automatycznie uaktualniane na wszystkich komputerach wchodzących w skład Systemu.
38. W przypadku wystąpienia awarii, operator musi otrzymywać powiadomienie na konto e-mail.
39. Możliwość uruchamiania zewnętrznych programów, skryptów lub plików wsadowych na serwerze backupu i na komputerach zdalnych przy użyciu [polecen](https://www.ferrobackup.com/pl/config.html#polecenia_lokalne) zdalnych I lokalnych;
40. Raporty zawierające dane podsumowujące przebieg archiwizacji, informacje na temat zaległych zadań archiwizacji oraz statystyki;
41. Mozliwość zabezpieczenia dokumentów z komputerów i serwerów NAS oraz samych kopii zapasowych przed programami szyfrującymi pliki typu ransomware;
42. [Pomoc techniczna w jęz. polskim](https://www.ferrobackup.com/pl/support.html) przez 36 miesięcy;
43. Czas reakcji serwisu – maksymalnie 48h *od poniedziałku do piątku w godzinach od 9.00 do 17.00*;
44. Forma - telefon, e-mail
45. Licencja nieograniczona czasowo;
46. Przedłużenie posiadanego przez zamawiającego oprogramowania antywirusowego na 35 stanowisk o kolejnych 36 miesięcy
47. **Serwer + macierz - zestaw – 1 szt.**
48. **Serwer**

|  |  |
| --- | --- |
| **Nazwa komponentu** | **Wymagane minimalne parametry techniczne**  |
| **Obudowa** | Obudowa Rack o wysokości maksymalnie 1U z możliwością instalacji do 4 dysków 3.5" wraz z kompletem szyn umożliwiających montaż w szafie rack. |
| **Płyta główna** | Zaprojektowana przez producenta serwera i oznaczona jego znakiem firmowym.Musi obsługiwać 128GB;4 sloty przeznaczone dla pamięci |
| Procesor | Osiągający w teście PassMark CPU Mark wynik 8 000 – **załączyć do oferty wydruk ze strony** [**https://www.cpubenchmark.net/**](https://www.cpubenchmark.net/) |
| **Pamięć RAM** | 32GB pamięci RAM ECC UDIMM o częstotliwości pracy 3200MT/s. |
| **Karta graficzna** | Zintegrowana karta graficzna umożliwiająca rozdzielczość min. 1280x1024 |
| **Wbudowane porty** | 4 porty USB w tym 1 x USB 3.01 port VGA 1 port RS232 |
| **Gniazda PCI** | 2 sloty PCIe generacji 4 |
| **Interfejsy sieciowe** | Wbudowane 2 interfejsy sieciowe 1Gb Ethernet w standardzie BaseT. Ilośćnie może być osiągnięta poprzez karty w slotach PCIe; |
| **Kontroler dysków** | Dedykowany sprzętowy kontroler dyskowy SAS 12Gb/s, umożliwiający konfiguracje poziomów RAID 0, 1, 10. Wsparcie dla dysków samoszyfujących.  |
| **Dyski twarde** | Możliwość instalacji dysków SAS, SATA, SSD, NL SASZainstalowane dyski:- 2 x SSD SATA o pojemności 960GB, 6Gbps, Hot-Plug.- 1 x HDD SATA o pojemności 2TB, 6Gbps, Hot-Plug.Możliwość zainstalowania dwóch dysków M.2 SATA o pojemności 480GB z możliwością konfiguracji RAID 1.Możliwość zainstalowania dedykowanego modułu dla hypervisora wirtualizacyjnego, wyposażonego w 2 nośniki typu flash o pojemności 64GB, z możliwością konfiguracji zabezpieczenia synchronizacji pomiędzy nośnikami z poziomu BIOS serwera.Rozwiązanie nie może powodować zmniejszenia ilości wnęk na dyski twarde. |
| **Zasilacze** | Zasilacz o mocymaksymalnie 450W, o sprawności 94% przy 50% obciążeniu zasilacza oraz o sprawności 90% przy 100% obciążeniu zasilacza.  |
| **Bezpieczeństwo** | * Zatrzask górnej pokrywy oraz blokada na ramce panela zamykana na klucz służąca do ochrony nieautoryzowanego dostępu do dysków twardych.
* Możliwość wyłączenia w BIOS funkcji przycisku zasilania.
* BIOS musi mieć możliwość przejścia do bezpiecznego trybu rozruchowego z możliwością zarządzania blokadą zasilania, panelem sterowania oraz zmianą hasła
* Wbudowany czujnik otwarcia obudowy współpracujący z BIOS i kartą zarządzającą.
* Moduł TPM 2.0
* Możliwość dynamicznego włączania I wyłączania portów USB na obudowie – bez konieczności restartu serwera
* Możliwość wymazania danych ze znajdujących się dysków wewnątrz serwera – niezależne od zainstalowanego systemu operacyjnego, uruchamiane z poziomu zarządzania serwerem
 |
| **Diagnostyka** | Na froncie obudowy panel LCD lub sygnalizacja diodami LED, umożliwiająca/-y wyświetlenie informacji o stanie: procesora, pamięci, dysków, BIOS’u, zasilaniu oraz temperaturze.  |
| **Karta Zarządzania** | Niezależna od zainstalowanego na serwerze systemu operacyjnego posiadająca dedykowany port Gigabit Ethernet RJ-45 i umożliwiająca:* monitoring wszystkich kluczowych komponentów (wentylatory, zasilacze, pamięć, procesor, RAID, karty sieciowe oraz dyski twarde)
* zdalny dostęp do graficznego interfejsu Web karty zarządzającej
* uzyskanie informacji o aktualnym zużyciu energii oraz temperaturach
* kontrola zasilania (włączenie, wyłączenie, restart)
* wsparcie dla IPv6
* funkcje diagnostyczne: podgląd dziennika systemowego, dziennika kontrolera cyklu życia;
* odtworzenie konfiguracji sprzętowej na podstawie kopii z innego serwera
* szyfrowanie protokołem SSL
* wsparcie dla dynamic DNS
 |
| System operacyjny | System operacyjny w najnowszej wersji spełniający poniższe wymagania: 1. Licencja musi uprawniać do uruchamiania serwerowego systemu operacyjnego (SSO) w środowisku fizycznym lub dwóch wirtualnych środowisk serwerowego systemu operacyjnego za pomocą wbudowanych mechanizmów wirtualizacji.
2. Możliwość migracji maszyn wirtualnych bez zatrzymywania ich pracy między fizycznymi serwerami z uruchomionym mechanizmem wirtualizacji (hypervisor) przez sieć Ethernet, bez konieczności stosowania dodatkowych mechanizmów współdzielenia pamięci.
3. Wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany pamięci RAM bez przerywania pracy.
4. Wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany procesorów bez przerywania pracy.
5. Automatyczna weryfikacja cyfrowych sygnatur sterowników w celu sprawdzenia, czy sterownik przeszedł testy jakości przeprowadzone przez producenta systemu operacyjnego.
6. Możliwość dynamicznego obniżania poboru energii przez rdzenie procesorów niewykorzystywane w bieżącej pracy. Mechanizm ten musi uwzględniać specyfikę procesorów wyposażonych w mechanizmy Hyper-Threading.
7. Wbudowany mechanizm klasyfikowania i indeksowania plików (dokumentów) w oparciu o ich zawartość.
8. Wbudowane szyfrowanie dysków przy pomocy mechanizmów posiadających certyfikat FIPS 140-2 lub równoważny wydany przez NIST lub inną agendę rządową zajmującą się bezpieczeństwem informacji.
9. Możliwość uruchamianie aplikacji internetowych wykorzystujących techologię ASP.NET.
10. Możliwość dystrybucji ruchu sieciowego HTTP pomiędzy kilka serwerów.
11. Wbudowana zapora internetowa (firewall) z obsługą definiowanych reguł dla ochrony połączeń internetowych i intranetowych.
12. Graficzny interfejs użytkownika.
13. Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, przeglądarka internetowa, pomoc, komunikaty systemowe.
14. Wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug&Play).
15. Możliwość zdalnej konfiguracji, administrowania oraz aktualizowania systemu.
16. Dostępność bezpłatnych narzędzi producenta systemu umożliwiających badanie i wdrażanie zdefiniowanego zestawu polityk bezpieczeństwa.
17. Pochodzący od producenta systemu serwis zarządzania polityką konsumpcji informacji w dokumentach (Digital Rights Management).
18. Możliwość implementacji następujących funkcjonalności bez potrzeby instalowania dodatkowych produktów (oprogramowania) innych producentów wymagających dodatkowych licencji:
19. Usługi sieciowe: DHCP oraz DNS wspierający DNSSEC.
20. Usługi katalogowe oparte o LDAP i pozwalające na uwierzytelnianie użytkowników stacji roboczych, bez konieczności instalowania dodatkowego oprogramowania na tych stacjach, pozwalające na zarządzanie zasobami w sieci (użytkownicy, komputery, drukarki, udziały sieciowe.
21. Zdalna dystrybucja oprogramowania na stacje robocze.
22. Praca zdalna na serwerze z wykorzystaniem terminala (cienkiego klienta) lub odpowiednio skonfigurowanej stacji roboczej.
23. PKI (Centrum Certyfikatów (CA), obsługa klucza publicznego i prywatnego) umożliwiające: dystrybucję certyfikatów poprzez http, konsolidację CA dla wielu lasów domeny, automatyczne rejestrowania certyfikatów pomiędzy różnymi lasami domen.
24. Szyfrowanie plików i folderów.
25. Szyfrowanie połączeń sieciowych pomiędzy serwerami oraz serwerami i stacjami roboczymi (IPSec).
26. Możliwość tworzenia systemów wysokiej dostępności (klastry typu fail-over) oraz rozłożenia obciążenia serwerów.
27. Serwis udostępniania stron WWW.
28. Wsparcie dla protokołu IP w wersji 6 (IPv6).
29. Wbudowane usługi VPN pozwalające na zestawienie nielimitowanej liczby równoczesnych połączeń i niewymagające instalacji dodatkowego oprogramowania na komputerac;,
30. Możliwość automatycznej aktualizacji w oparciu o poprawki publikowane przez producenta wraz z dostępnością bezpłatnego rozwiązania producenta SSO umożliwiającego lokalną dystrybucję poprawek zatwierdzonych przez administratora, bez połączenia z siecią Internet.
31. Wsparcie dostępu do zasobu dyskowego SSO poprzez wiele ścieżek (Multipath);
32. Możliwość instalacji poprawek poprzez wgranie ich do obrazu instalacyjnego.
33. Mechanizmy zdalnej administracji oraz mechanizmy (również działające zdalnie) administracji przez skrypty.
34. Możliwość zarządzania przez wbudowane mechanizmy zgodne ze standardami WBEM oraz WSManagement organizacji DMTF;
35. Materiały edukacyjne w języku polskim.
36. Licencja na 16 rdzeni procesorowych;
37. Analizator najlepszych praktyk
38. Pamięć dynamiczna przy wirtualizacji;
39. Dodawanie i wymiana kości RAM bez wyłączania systemu operacyjnego;
40. Konsola zarządzająca;
41. Sieciowy load balancing;
42. Migracja pamięci masowej;
43. Aktywacja zbiorcza;
44. Manager zasobów systemu operacyjnego;
45. Logowanie licencji serwera;
46. Nieograniczona liczba połączeń RRAS;
47. Trzydzieści licencji dostępowych dla użytkowników sieciowych w sieci LAN zamawiającego;
48. Obsługa 64 gniazd 64 bitowych;
49. Obsługa 24 TB pamięci RAM;
50. Możliwość dołączenia do domeny;
51. Kodeki DLNA i strumieniowe przesyłanie multimediów internetowych;
52. Certyfikaty usług katalogowych;
53. Zarządzanie usługami katalogowymi;
54. Serwer: DHCP, DNS, iPAM, iSNS, SMTP, faksów, plików, dla NFS;
55. Deduplikacja danych
56. Replikacja systemu plików DFS;
57. Funkcja serwera docelowego iSCSI I kontrolera sieci;
58. Możliwość dostępu i pulpitu zdalnego;
59. Usługi IIS;
60. Usługa inteligentnego transferu w tle;
61. Szyfrowanie I odblokowywanie dysków bitlocker;
62. Możliwość pracy w klastrze;
63. Zarządzanie politykami grupowymi;
64. Monitorowanie portów LPR;
65. Kolejkowanie wiadomości;
66. Protokół rozpoznawania nazw równorzędnych;
67. Manager połączeń RAS;
68. Zdalna pomoc użytkownikom sieciowym;
69. Zdalna kompresja różnicowa;
70. RSAT;
71. RPC przez proxy HTTP;
72. Usługi TCP/IP;
73. Udostępnianie plików SMB 1.0/CIFS;
74. Klient Telnet i TFTP;
75. Wewnętrzna baza danych;
76. Kopia zapasowa serwera;
77. Narzędzia do migracji system operacyjnego;
78. Filtr TIFF IF;
 |
| Oprogramowanie zabezpieczające | System chroniący przed zagrożeniami, posiadający certyfikaty VB100%, OPSWAT, AVLAB +++, AV Comperative Advance + musi umożliwiać co najmniej:1. Wykrywanie i blokowania plików ze szkodliwą zawartością, w tym osadzonych/skompresowanych plików, które używają czasie rzeczywistym algorytmów kompresji,
2. Wykrywanie i usuwanie plików typu rootkit oraz złośliwego oprogramowania, również przy użyciu technik behawioralnych,
3. Stosowanie kwarantanny
4. Wykrywanie i usuwanie fałszywego oprogramowania bezpieczeństwa (roguewear)
5. Skanowanie urządzeń USB natychmiast po podłączeniu,
6. Automatyczne odłączanie zainfekowanej końcówki od sieci,
7. Skanowanie plików w czasie rzeczywistym, na żądanie, w interwałach czasowych lub poprzez harmonogram, w sposób w pełni konfigurowalny w przypadku wykrycia zagrożenia, z możliwością wykluczenia typu pliku lub lokalizacji.
8. Zarządzanie stacją kliencką poprzez zbieranie informacji co najmniej o: nazwie, producencie i modelu komputera, przynależności do grupy roboczej/domeny, szczegółach systemu operacyjnego, lokalnych kontach użytkowników, dacie i godzinie uruchomienia i ostatniego restartu komputera, parametrach sprzętowych (procesor, RAM, SN, dysk), BIOS, interfejsach sieciowych, dołączonych peryferiach.
9. Musi posiadać moduł ochrony IDS/IPS
10. Musi posiadać mechanizm wykrywania skanowania portów
11. Musi pozwalać na wykluczenie adresów IP oraz PORTów TCP/IP z modułu wykrywania skanowania portów
12. Moduł wykrywania ataków DDoS musi posiadać kilka poziomów wrażliwości
13. Oprogramowanie do szyfrowania, chroniące dane na stacji za pomocą algorytmów szyfrowania takich jak AES, RC6, SERPENT i DWAFISH.
14. Pełne szyfrowanie dysków działających w oferowanych komputerach zapobiegające utracie danych z powodu utraty / kradzieży stacji roboczej.
15. Oprogramowanie musi szyfrować całą zawartość na urządzeniach przenośnych, takich jak pendrive, dyski USB i udostępniać ją tylko autoryzowanym użytkownikom.
16. Musi umożliwiać blokowanie wybranych przez administratora urządzeń zewnętrznych podłączanych do stacji;
17. Musi umożliwiać zdefiniowanie listy zaufanych urządzeń, które nie będą blokowane podczas podłączanie do stacji.
18. Możliwość blokady zapisywania plików na zewnętrznych dyskach USB oraz możliwości uruchamiania oprogramowania z takich dysków. Blokada ta musi umożliwiać korzystanie z pozostałych danych zapisanych na takich dyskach.
19. Interfejs zarządzania musi wyświetlać monity o zbliżającym się zakończeniu licencji, a także powiadamiać o zakończeniu licencji.
20. Moduł chroniący dane użytkownika przed działaniem oprogramowania ransomware poprzez ograniczenie możliwości modyfikowania chronionych plików, tylko do procesów systemowych oraz zaufanych aplikacji.
21. Możliwość zdefiniowania chronionych folderów zawierających wrażliwe dane użytkownika.
22. Możliwość zdefiniowania zaufanych folderów. Aplikacje uruchamiane z zaufanych folderów mają możliwość modyfikowania plików objętych ochroną any ransomware.
23. Monitorowanie krytycznych danych użytkownika zapobiegające atakom ransomware;
24. Centralna konsola zarządzająca umożliwiająca co najmniej:
25. przechowywanie danych w bazie typu SQL
26. zdalną instalację lub deinstalację oprogramowania, na pojedynczych stacjach, zakresie adresów IP lub grupie z ActiveDirectory;
27. tworzenie paczek instalacyjnych oprogramowania, z rozróżnieniem docelowej platformy systemowej (w tym 32 lub 64bit dla systemów Windows i Linux), w formie plików .exe lub .msi oraz formatach dla systemów Linux
28. centralną dystrybucję uaktualnień definicji ochronnych, których źródłem będzie plik na serwerz konsoli;
29. raportowanie z prezentacją tabelaryczną i graficzną, możliwością automatycznego czyszczenia starych raportów, eksportu do formatów CSV i PDF, prezentujące dane zarówno z logowania zdarzeń serwera konsoli, jak i raporty zbierane ze stacji klienckich, w tym raporty o oprogramowaniu zainstalowanym na stacjach klienckich;
30. definiowanie struktury opartej o role i polityki, w których każda z funkcjonalności musi mieć możliwość konfiguracji;
31. Możliwość tworzenia kopii zapasowych i przywracania plików konfiguracyjnych z serwera;
32. Dostęp do konsoli z dowolnego miejsca w nagłych przypadkach;
33. Możliwość przeglądania raportów podsumowujących dla wszystkich urządzeń
34. Centralna konsola do zarządzania i monitorowania użycia zaszyfrowanych woluminów dyskowych, dystrybucji szyfrowania, polityk i centralnie zarządzanie informacjami odzyskiwania, niezbędnymi do uzyskania dostępu do zaszyfrowanych danych w nagłych przypadkach.
35. Aktualizacja oprogramowania w trybie offline, za pomocą paczek aktualizacyjnych;
36. System musi umożliwiać, z konsoli na serwerze, co najmniej:
37. różne ustawienia dostępu dla urządzeń: pełny dostęp, tylko do odczytu i blokowanie
38. przyznawanie praw dostępu dla nośników pamięci tj. USB, CD
39. regulowania połączeń WiFi i Bluetooth
40. kontrolowanie i regulowanie użycia urządzeń peryferyjnych typu: drukarki, skanery i kamery internetowe
41. blokadę lub zezwolenia na połączenie się z urządzeniami mobilnymi
42. blokowanie dostępu dowolnemu urządzeniu
43. tymczasowe dodanie dostępu do urządzenia przez administratora
44. szyfrowanie zawartości USB i udostępnianie jej na stacjach końcowych;
45. zablokowanie funkcjonalności portów USB, blokując dostęp urządzeniom innym niż klawiatura i myszk
46. zezwalanić na dostęp tylko urządzeniom wcześniej dodanym przez administratora
47. używanda tylko zaufanych urządzeń sieciowych;
48. Funkcja wirtualnej klawiatury
49. Możliwość blokowania każdej aplikacji , w tym w oparciu o kategorie
50. Możliwość dodania własnych aplikacji do listy zablokowanych
51. Tworzenie listy aplikacji zainstalowanych na komputerach klientach poprzez konsolę administracyjną na serwerze
52. Kategorie aplikacji typu: tuning software, toolbars, proxy, network tools, file sharing application, backup software, encrypting tool
53. Możliwość generowania i wysyłania raportów o aktywności na różnych kanałach transmisji danych, takich jak wymienne urządzenia, udziały sieciowe czy schowki;
54. Możliwość zablokowania funkcji Printscreen
55. Monitorowanie przesyłu danych między aplikacjami;
56. Monitorowanie i kontrola przepływu poufnych informacji
57. Blokowanie plików w oparciu o ich rozszerzenie lub rodzaj
58. Monitorowanie i zarządzanie danymi udostępnianymi poprzez zasoby sieciowe;
59. Ochrona przed wyciekiem informacji na drukarki lokalne i sieciowe
60. Ochrona zawartości schowka systemu
61. Ochrona przed wyciekiem informacji w poczcie e-mail w komunikacji SSL
62. Dodawanie wyjątków dla domen, aplikacji i lokalizacji sieciowych
63. Ochrona plików zamkniętych w archiwach
64. Zmiana rozszerzenia pliku nie może mieć znaczenia w ochronie plików przed wyciekiem
65. Możliwość tworzenia profilu DLP dla każdej polityki
66. Wyświetlanie alertu dla użytkownika w chwili próby wykonania niepożądanego działania
67. Ochrona przez wyciekiem plików poprzez programy typu p2p
68. Monitorowanie działań związanych z obsługą plików, takich jak kopiowanie, usuwanie, przenoszenie na dyskach lokalnych, dyskach wymiennych i sieciowych.
69. Monitorowanie określonych rodzajów plików.
70. Możliwość wykluczenia określonych plików/folderów z procedury monitorowania.
71. Możliwość śledzenia zmian we wszystkich plikac
72. Możliwość śledzenia zmian w oprogramowaniu zainstalowanym na stacjach roboczych;
73. Możliwość definiowana własnych typów plików
74. Usuwanie tymczasowych plików, czyszczenie niepotrzebnych wpisów do rejestru oraz defragmentacji dysku
75. Optymalizacja w chwili startu systemu operacyjnego, przed jego całkowitym uruchomieniem
76. Możliwość zaplanowania optymalizacji na wskazanych stacjach klienckich
77. System ochrony i zarządzania urządzeniami za pomocą platformy w chmurze;.
78. Musi posiadać możliwość sprawdzenia listy urządzeń przypisanych użytkownikowi
79. Musi posiadać możliwość eksportu danych użytkownika
80. Import listy urządzeń z pliku CSV
81. Dodawanie urządzeń;
82. Podgląd co najmniej następujących informacji konfiguracji: data i status wdrożenia, status urządzenia, numer telefonu, właściciel, grupa, reguły, wersja agenta
83. Podgląd co najmniej następujących informacji sprzętowych: model, producent, system, adres MAC, bluetooth, wolna przestrzeń na dysku, całkowita przeszłość na dysku, użycie procesora,;
84. Podgląd zainstalowanych aplikacji;
85. Moduł raportowania aktywności, skanowania oraz naruszenia reguł;
86. Oprogramowanie pozwalające na wykrywanie oraz zarządzanie podatnościami bezpieczeństwa dostępne przez przeglądarkę internetową;
87. Portal zarządzający w postaci SaaS;
88. Skanowanie podatności za pomocą nodów skanujących;
89. Nody skanujące w postaci usługi hostowanej na serwerach producenta oraz w postaci aplikacji instalowanej lokalnie
90. Portal zarządzający musi umożliwiać:
91. przegląd wybranych danych;
92. zablokowanie możliwości zmiany konfiguracji;
93. zarządzanie skanami podatności (start, stop), przeglądanie listy podatności oraz tworzenie raportów;
94. tworzenie grup skanów z odpowiednią konfiguracją poszczególnych skanów podatności
95. eksport skanów podatności do pliku CSV;
96. **D**eduplikacja danych na źródle,
97. Backup przyrostowy i różnicowy,
98. Wersjonowanie plików – możliwość zdefiniowania dowolnej ilości wersji,
99. Backup danych lokalnych – plikowy oraz poczty;
100. Backup otwartych plików;
101. Filtr plików oraz folderów,
102. Domyślne wykluczenia zbędnych plików;
103. Wyłączanie komputera po wykonaniu backup;
104. Przywracanie danych do wskazanej lokalizacji,
105. Możliwość backup-u z wykorzystaniem dowolnej ilości rdzeni procesora,
106. Wyszukiwanie plików w repozytorium użytkownika,
107. Automatyczne logowanie,
108. Zapamiętywanie danych logowania,
109. Automatyczne uruchamianie programu przy starcie systemu,
110. Ustawianie priorytetu dla procesu backupu,
111. Zmiana klucza szyfrującego,
112. Ustawienia przepustowości/zajętości pasma,
113. Konfiguracja wydajności procesu backupu,
114. Zastępowanie nazwy pliku GUID-em,
115. Szyfrowanie danych algorytmem AES 256 CBC;
116. Kompresja danych,
117. Deklaracja klucza szyfrującego dane użytkownika,
118. Szczegółowy dziennik zdarzeń dostępny z poziomu aplikacji,
119. Obliczanie sumy kontrolnej,
120. Licencje z przestrzenią w chmurze –50 GB.
121. Wsparcie techniczne, świadczone przez producenta, w języku polskim;
 |
| Certyfikaty | Serwer musi znajdować się na ogólnodostępnej liście producenta oferowanego systemu operacyjnego, potwierdzającej kompatybilnośc oferowanego sprzętu i oprogramowania- **załączyć do oferty wydruk ze strony;**Serwer musi pochodzić z autoryzowanego kanału sprzedaży producenta na rynek polski – **załaczyć do oferty oświadczenie producenta;** |
| Warunki gwarancji | 3 lata gwarancji, z czasem reakcji do następnego dnia roboczego od przyjęcia zgłoszenia;Możliwość zgłaszania awarii 24x7x365 poprzez ogólnopolską linię telefoniczną producenta. Możliwość rozszerzenia gwarancji przez producenta do 5 lat;Możliwość sprawdzenia statusu gwarancji poprzez stronę producenta podając unikatowy numer urządzenia oraz pobieranie uaktualnień mikrokodu oraz sterowników nawet w przypadku wygaśnięcia gwarancji serwera |
| Dokumentacja użytkownika | Zamawiający wymaga dokumentacji w języku polskim lub angi*e*lskim.Możliwość telefonicznego sprawdzenia konfiguracji sprzętowej serwera oraz warunków gwarancji po podaniu numeru seryjnego bezpośrednio u producenta lub jego przedstawiciela. |

1. **Macierz**

|  |  |
| --- | --- |
| **Nazwa komponentu** | **Wymagane minimalne parametry techniczne**  |
| Procesor |  Musi osiagać wynik 3450 wteście Average CPU Mark – **załączyć do**  **oferty wydruk ze strony** [**www.cpunechmark.net**](http://www.cpunechmark.net) **lub** [**www.passmark.com**](http://www.passmark.com) |
| Pamięć | 2 GB; |
| Kieszenie na dyski | 4 szt.; |
| Obsługiwane dyski | 2,5 i 3,5 cala HDD i SSD, hot swap; |
| Porty | 2 z 1 GbE z obsługą funkcji Link Aggregation; 1 x USB 3.2;1 x PCIe Gen.3 |
| Wspierane systemy plików | Btrfs, EXT4; |
| Obudowa | Rack maksymalnie 1U z szynami montażowymi w szafie; |
| Wentylacja | 3 wentylatory o rozmiarze 40 x 40 mm, pracujące w trybie pełnej prędkości, chłodzenia i cichym; |
| Głośność | Maksymalnie 30 dB; |
| Zasilacz | Maksymalnie 100W; |
| Zainstalowane dyski | 4 x 12 TB SATA 6 Gb/s 7200 rpm, przeznaczone do pracy w trybie ciągłym w serwerach NAS;MTBF – 1 mln. godzin, Głośność podczas pracy – maksymalnie 3 bele;Gwarancja – 3 lata;Pobór pradu podczas pracy – maksymalnie 8W; |
| Zużycie energii | Maksymalnie 40W w trybie dostępu do danych; |
| System operacyjny | * 1. Obsługa zbiorczego tworzenia użytkowników przez importowanie list użytkowników;
	2. Obsługa dodawania użytkowników do więcej niż jednej grupy użytkowników;
	3. Obsługa konfiguracji siły hasła i reguł wygaśnięcia
	4. Możliwość samodzielnego resetowania hasła w przypadku użytkowników niebędących administratorami
	5. Możliwość dostosowania uprawnień dla poszczególnych folderów i plików dla użytkowników i grup
	6. Możliwość dostosowania ustawień uprawnień aplikacji dla użytkowników, grup i adresów IP
	7. Obsługa limitów konfiguracji wolumenów/folderów współdzielonych w celu kontrolowania maksymalnej ilości miejsca dostępnego dla każdego użytkownika
	8. Obsługa limitów szybkości dla użytkowników i grup dla protokołów FTP;
	9. SSD TRIM;
	10. Wparcie dla RAID 0,1,5,6,10, JBOD;
	11. Migracja z RAID 1 do 5 i z 5 do 6;
	12. Możliwość powiększenia wolumenu przez dodanie kolejnych dysków lub zamianę dysków mniejszych na większe;
	13. Obsługa FTP, FTP przez SSL/TLS i SFTP;
	14. Ustawienia limitu czasu rozłączania bezczynnych użytkowników
	15. Mozliwość dostosowania zakresów portów dla pasywnych połączeń FTP;
	16. Transfer plików między serwerami;
	17. Ustawienia ograniczeń połączeń dla adresów IP
	18. Ustawienia limitu prędkości dla określonych użytkowników lub grup;
	19. Obsługa trybu transferu ASCII
	20. Obsługa kodowania UTF-8 dla plików z wielojęzycznymi nazwami
	21. Katalog główny dla każdego użytkownika
	22. Anonimowy FTP;
	23. Obsługa protokołu SSH podczas przesyłania plików;
	24. Synchronizacja folderów współdzielonych;
	25. Kopia zapasowa jednostek LUN
	26. Zarządzanie pamięcią masową i monitorowanie użycia pamięci masowej serwera;
	27. Obsługa deduplikacji danych w celu optymalizacji;
	28. Obsługa pamięci podręcznej SSD w celu zwiększenia wydajności systemu;
	29. Przeglądanie migawek tylko do odczytu
	30. Menedżer plików do przeglądania i zarządzania folderami i plikami przechowywanymi na serwerze;
	31. Bezpieczne udostępnianie plików
	32. Dostęp i zarządzanie z komputerów osobistych, tabletów i telefonów komórkowych;
	33. Montowanie dysków wirtualnych, folderów zdalnych i pamięci masowej w chmurze publicznej;
	34. Odzyskiwanie lub pobieranie usuniętych plików z kosza
	35. Wyświetlanie i dostosowywanie uprawnień ACL do plików i folderów;
	36. Obsługa edytora ACL
	37. Dostosowywanie atrybutów folderów współdzielonych do wyświetlania;
	38. Kompresowanie lub wyodrębnianie zarchiwizowanych plików i folderów;
	39. Montowanie dysków wirtualnych w celu uzyskania dostępu do zawartości plików obrazów dysków (.iso
	40. Montowanie folderów zdalnych ze zdalnych serwerów obsługujących protokoły SMB1/SMB2/SMB3/NFS
	41. Łączenie ze zdalnymi usługami chmury publicznej i serwerami plików;
	42. Obsługiwane protokoły: FTP, SFTP, WebDAV, WebDAV HTTPS
	43. Centralne zarządzanie za pośrednictwem menedżera łączy udostępnionych;
	44. Logi transferu plików i działań użytkownika z możliwościa eksportu;
 |
| Warunki gwarancji | 3 lata; |
| Wymagania dodatkowe | Możliwość zaplanowania włączenia oraz wyłączenia, funkcja Wake on LAN / WAN; |

1. **Serwer kopii zapasowej – 2 szt**.

|  |  |
| --- | --- |
| **Nazwa komponentu** | **Wymagane minimalne parametry techniczne**  |
| Procesor |  Musi osiagać wynik 1940 wteście Average CPU Mark – **załączyć do**  **oferty wydruk ze strony** [**www.cpunechmark.net**](http://www.cpunechmark.net) |
| Pamięć | 2 GB zmożliwościa rozszerzenia do 6 GB; |
| Kieszenie na dyski | 6 szt. w 2 szt. na NVMe; |
| Obsługiwane dyski | 2,5 i 3,5 cala HDD i SSD, M.2 2280 NVMe SSD, hot swap; |
| Porty | 2 z 1 GbE z obsługą funkcji Link Aggregation; 2 x USB 3.2; |
| Wspierane systemy plików | Btrfs, EXT4; |
| Obudowa | Rack lub tower; |
| Wentylacja | 2 wentylatory o rozmiarze 90 x 90 mm, pracujące w trybie pełnej prędkości, chłodzenia i cichym; |
| Głośność | Maksymalnie 20 dB; |
| Zasilacz | Maksymalnie 100W; |
| Zainstalowane dyski | 4 x 12 TB SATA 6 Gb/s 7200 rpm, przeznaczone do pracy w trybie ciągłym w serwerach NAS;MTBF – 1 mln. godzin, Głośność podczas pracy – maksymalnie 3 bele;Gwarancja – 3 lata;Pobór pradu podczas pracy – maksymalnie 8W; |
| Zużycie energii | Maksymalnie 30W w trybie dostępu do danych; |
| System operacyjny | * 1. Obsługa zbiorczego tworzenia użytkowników przez importowanie list użytkowników;
	2. Obsługa dodawania użytkowników do więcej niż jednej grupy użytkowników;
	3. Obsługa konfiguracji siły hasła i reguł wygaśnięcia
	4. Możliwość samodzielnego resetowania hasła w przypadku użytkowników niebędących administratorami
	5. Możliwość dostosowania uprawnień dla poszczególnych folderów i plików dla użytkowników i grup
	6. Możliwość dostosowania ustawień uprawnień aplikacji dla użytkowników, grup i adresów IP
	7. Obsługa limitów konfiguracji wolumenów/folderów współdzielonych w celu kontrolowania maksymalnej ilości miejsca dostępnego dla każdego użytkownika
	8. Obsługa limitów szybkości dla użytkowników i grup dla protokołów FTP;
	9. SSD TRIM;
	10. Wparcie dla RAID 0,1,5,6,10, F1,JBOD;
	11. Konwersja z RAID 1 do 5 i z 5 do 6, SHR-1 na SHR-2;
	12. Obsługa FTP, FTP przez SSL/TLS i SFTP;
	13. Ustawienia limitu czasu rozłączania bezczynnych użytkowników
	14. Mozliwość dostosowania zakresów portów dla pasywnych połączeń FTP;
	15. Transfer plików między serwerami;
	16. Ustawienia ograniczeń połączeń dla adresów IP
	17. Ustawienia limitu prędkości dla określonych użytkowników lub grup;
	18. Obsługa trybu transferu ASCII
	19. Obsługa kodowania UTF-8 dla plików z wielojęzycznymi nazwami
	20. Katalog główny dla każdego użytkownika
	21. Anonimowy FTP;
	22. Obsługa protokołu SSH podczas przesyłania plików;
	23. Synchronizacja folderów współdzielonych;
	24. Kopia zapasowa jednostek LUN
	25. Zarządzanie pamięcią masową i monitorowanie użycia pamięci masowej serwera;
	26. Obsługa deduplikacji danych w celu optymalizacji;
	27. Obsługa pamięci podręcznej SSD w celu zwiększenia wydajności systemu;
	28. Przeglądanie migawek tylko do odczytu
	29. Menedżer plików do przeglądania i zarządzania folderami i plikami przechowywanymi na serwerze;
	30. Bezpieczne udostępnianie plików
	31. Dostęp i zarządzanie z komputerów osobistych, tabletów i telefonów komórkowych;
	32. Montowanie dysków wirtualnych, folderów zdalnych i pamięci masowej w chmurze publicznej;
	33. Odzyskiwanie lub pobieranie usuniętych plików z kosza
	34. Wyświetlanie i dostosowywanie uprawnień ACL do plików i folderów;
	35. Obsługa edytora ACL
	36. Dostosowywanie atrybutów folderów współdzielonych do wyświetlania;
	37. Kompresowanie lub wyodrębnianie zarchiwizowanych plików i folderów;
	38. Montowanie dysków wirtualnych w celu uzyskania dostępu do zawartości plików obrazów dysków (.iso
	39. Montowanie folderów zdalnych ze zdalnych serwerów obsługujących protokoły SMB1/SMB2/SMB3/NFS
	40. Łączenie ze zdalnymi usługami chmury publicznej i serwerami plików;
	41. Obsługiwane protokoły: FTP, SFTP, WebDAV, WebDAV HTTPS
	42. Centralne zarządzanie za pośrednictwem menedżera łączy udostępnionych;
	43. Logi transferu plików i działań użytkownika z możliwościa eksportu;
 |
| Warunki gwarancji | 3 lata; |
| Wymagania dodatkowe | Możliwość zaplanowania włączenia oraz wyłączenia, funkcja Wake on LAN / WAN, kontrolki LED zregulacja jasności, przywracanie zasilania; |

1. **Zasilacz awaryjny – zestaw - 2 szt.**

|  |  |
| --- | --- |
| **Nazwa komponentu** | **Wymagane minimalne parametry techniczne** |
| Rodzaj |  jednofazowy |
| Typ obudowy | Metalowa tower/rack 2U z zestawem montażwym w szafie rack; |
| Topologia | podwójna konwersja online |
| Rodzaj wejścia | IEC C20; |
| Wyjście | 8 x IEC C13 zabezpieczone przed przepięciami i bateriami; |
| Obciązenie krytyczne i niekrytyczne CL/NCL | 4/4 |
| Współczynnik mocy/szczytu | 0,9 / 3:1; |
| Czas transferu | 0 ms. |
| Przewód zasilający | 1,8 m. |
| Moc wyjściowa VA/W | 2000/1800 |
| Układ przecieprzepięciowy | 400J, ochrona sieci LAN (RJ45),  |
| Czas pracy na baterii (podtrzymania) | 5 minut przy pełnym obciążeniu/ 15 min. przy połowicznym; |
| Typowy czas ładowania baterii | Maksymalnie 4h; |
| Głośność | Maksymalnie 45 dBA; |
| Moduł bateryjny | Napięcie wyjściowe – 70V;Liczba baterii – 12 szt.Typowy czas ponownego ładowania – 2h;Możliwość wymiany przez użytkownika i rozbudowy;Host swap;Obudowa metalowa rack/tower 2U z szynami rack; |
| Zdalne zarządzani | Przeglądarka internetowa, wiersz poleceń, NMS;Obsługiwane protokoły - IPv4/v6, SNMPv1/v3, HTTP/HTTPs, TCP/IP, UDP, DHCP, NTP, DNS, SMTP, SSH, SSL, TLS, Telnet, FTP i SyslogUwierzytelnianie - RADIUS, LDAP, LDAPS;Obsluga czujnika środowiskowego;Powiadomienia o wydarzeniach - E-mail, komunikaty SNMP, Syslog, SMS |
| Złącza | 1 x RS232, 1 x USB, 3 x RJ45, 1 x RJ11, 1 x EPO; |
| Warunki gwarancji | 3 lata; |
| Wymagania dodatkowe | Kompatybilność z aktywnym PFC i generatoremmożliwośc konfiguracji napięcia wyjściowego, automatyczne wykrywanie częstotliwości wejściowej i możliwość konfiguracji wyjściowej, ochrona przed przeciążeniem w trybie liniowym i obejsciowym, wewnętrzny ogranicznik prądu, bezpiecznik, automatyczne i ręczne wewnętrzne obejscie, uruchamianie na baterii, bateria hot swap z możliwością samodzielnej wymiany przez użytkownika, mozliwośc podłączenie 3 zewnetrznych modułów bateryjnych, filtrowanie EMI/RFI, kabel USB, 2 x przewód zasilający, panel LCD; |

1. **Wdrożenie;**

W ramach wdrożenia wykonawca będzie zobowiązany do wykonania następującego zakresu prac:

1. Integracja urządzeń z infrastrukturą zamawiającego
2. Przeszkolenie indywidulane wskazanych przez Zamawiającego pracowników urzędu z obsługi dostarczonych urządzeń;
3. Instalacja Szafy serwerowej Rack, w tym:
4. Instalacja 2 szt. Pólek do szafy rac
5. Instalacja panelu wentylatorów dedykowanych do szafy rack
6. Instalacja i konfiguracja zasilacza awaryjnego wraz z modułem baterii
7. Instalacja 2 szt listew zasilających wraz z wyłącznikiem
8. Instalacja 6 szt Patch paneli RJ-45 Kat 6
9. Połączenie zainstalowanych patch paneli z istniejącym okablowaniem Zamawiającego.
10. Montaż zakupionych urządzeń w szafie serwerowej RACK oraz uporządkowanie/organizacja okablowania i spięcie urządzeń kablami sieciowymi
11. Instalacja serwera DELL PowerEdge R250w tym:
12. Aktualizacja sterowników do podzespołów oraz BIOS serwera;
13. Instalacja i konfiguracja oprogramowania serwerowego,  w tym systemu operacyjnego,
14. Konfiguracja zabezpieczeń
15. Konfiguracja usług aktualizacyjnych
16. Instalacja i konfiguracja serwera NAS przeznaczonego do wykorzystania jako repozytorium danych w tym:
17. Instalacja dysków w obudowie serwera
18. Konfiguracja dysków logicznych
19. Konfiguracja zabezpieczeń
20. Konfiguracja reguł udostępniania utworzonych wolumenów
21. Instalacja i konfiguracja serwera NAS przeznaczonego do systemu backup
22. Instalacja dysków w obudowie serwer
23. Konfiguracja dysków logicznyc
24. Konfiguracja zabezpiecze
25. Konfiguracja reguł udostępniania utworzonych wolumenów
26. Instalacja i konfiguracja systemu backup dla 2 serwerów i 30 stacji roboczych, w tym
27. Instalacja systemu serwerowego na wskazanej przez Zamawiającego maszynie.
28. Instalacja oprogramowania klienckiego na backupowanych końcówkach
29. Wykonanie planu kopii zapasowych stanowisk komputerowych
30. Konfiguracja zabezpieczeń
31. Instalacja i konfiguracja przełączników zarządzalnych oraz pozostałych urządzeń sieciowych w tym:
32. Konfiguracja usług;
33. Konfiguracja zabezpieczeń
34. Wydzielenie podsieci VLAN zgodnie z wymaganiami Zamawiającego
35. Stworzenie dokumentacji techniczno-eksploatacyjnej
36. Opis architektury technicznej (komponentów sprzętowych, systemowych)
37. Opis i schemat architektury logicznej (powiązań poszczególnych komponentów i ich rolę w architekturze)
38. Opis i instrukcja instalacji oraz konfiguracji wdrożonych komponentów sprzętowych, systemowych
39. Dokumentacja administracyjna związana z poprawną eksploatacja
40. **Szkolenie w zakresie cyberbezpiecześńtwa**

**1. Przedmiot zamówienia**

Szkolenie z zakresu bezpieczeństwa teleinformatycznego dla 25 pracowników biurowych Zamawiającego, podzielonych na 2 grupy.

**2. Zakres merytoryczny szkolenia**

Główny cel szkolenia to zbudowanie świadomości zagrożeń oraz umiejętności przeciwdziałania im we współczesnym cyberświecie.

**3. Czas trwania szkolenia:**

3 h na grupę. Przeszkolone zostaną 2 grupy

**4. Program szkolenia:**

Szkolenie zaznajomi uczestników z zagrożeniami, technikami ataków cyberprzestępczych oraz metodami socjotechnicznymi, ukierunkowanymi na osoby pracujące na co dzień przed komputerem.

1. Co to jest cyberprzestępczość
2. Opis funkcjonowania zorganizowanych grup cyberprzestępczych
3. Czy naprawdę nam zagrażają
4. Czy jestem atrakcyjnym „klientem” dla cyberprzestępcy
5. Jakie zyski może mieć cyberprzestępca atakując moje dane
6. Straty wynikające z udanego ataku na instytucję
7. Rodzaje ataków skierowane w pracowników biurowych
8. Jak cyberprzestępca dołącza nasz komputer do sieci Botnet
9. Jak się przed tym bronić
10. Spam jako niegroźny sposób na groźne ataki
11. Handel adresami e-mail
12. Kampanie Phishingowe jako metoda okradania kont bankowych
13. Opłacalność ataków DoS/DDoS wymierzonych w naszą instytucję
14. Groźne ataki 0-day - czy istnieje sposób obrony przed nimi
15. Nieopłacona FV jako sposób przemycenia wirusa do naszego systemu
16. Skąd cyberprzestępca zna moje hasło
17. Skanowanie kart płatniczych - gdzie i kiedy ktoś zeskanował moja kartę
18. Ataki socjotechniczne - czyli niewinne „wyłudzanie” danych
19. Przekazywanie haseł dostępowych współpracownikom
20. Fizyczne bezpieczeństwo miejsca pracy
21. Znaleziony pendrive jako pozwolenie na atak dla cyberprzestępcy

**5. Forma szkolenia:** stacjonarne w siedzibie Zamawiającego;

**6. Materiały szkoleniowe:**

Materiały szkoleniowe dla uczestników, w formie PDF lub prezentacji PowerPoint.

**7. Zaświadczenia ukończenia szkolenia.**

Zostaną przygotowane zgodnie z wytycznymi Zamawiającego na podstawie przesłanych list uczestników;

Będą zawierały imię i nazwisko uczestnika, tytuł wskazujący na realizowany program szkolenia i informację o jego terminie;

8. **Wsparcie poszkoleniowe trenera**

Wykonawca zapewni uczestnikom 14 dniowy kontakt z trenerem po szkoleniu.