Zał. Nr 1 do SWZ

**OPIS PRZEDMIOTU ZAMÓWIENIA**

Dotyczy: postępowania o wartości powyżej 170 000 zł w trybie podstawowym bez negocjacji (art. 275 pkt 1 ustawy PZP) pn **„Cyberbezpieczny Samorząd dla Miasta i Gminy Wodzisław.”**

dofinansowanego z programu Fundusze Europejskie na Rozwój Cyfrowy 2021-2027 (FERC),

Podane poniżej parametry sprzętu i oprogramowania są minimalnymi parametrami wymaganymi przez Zamawiającego. Zamawiający dopuszcza dostawę sprzętu i oprogramowania o parametrach lepszych niż wskazane poniżej pod warunkiem, że wszystkie minimalne parametry wskazane przez Zamawiającego będą spełnione.

Zamawiający wymaga aby dostarczony sprzęt był fabrycznie nowy, nieużywany, nieregenerowany, kompletny, dostarczony w oryginalnych opakowaniach. Zamawiający dopuszcza, by sprzęt został rozpakowany i uruchomiony przed jego dostarczeniem wyłącznie przez Wykonawcę i wyłącznie w celu weryfikacji działania sprzętu. Nie dopuszcza się zastosowania sprzętu tzw. „refurbished”. Dostarczany sprzęt musi być sprawny technicznie i pochodzić z autoryzowanego kanału dystrybucyjnego.

Zamawiający wymaga aby dostarczane oprogramowanie było nowe, nieużywane, nieaktywowane wcześniej na innym urządzeniu, dostarczone w najnowszej stabilnej wersji pochodzącej z oficjalnego kanału dystrybucyjnego producenta oprogramowania nieobciążone prawami na rzecz osób trzecich. Zamawiający zastrzega sobie prawo do przeprowadzenia weryfikacji oryginalności dostarczanego oprogramowania u jego producenta/dystrybutora.

Dostarczany sprzęt jak i oprogramowanie musi być wolny od wszelkich wad prawnych i fizycznych, w tym roszczeń osób trzecich oraz zajęć egzekucyjnych. Wykonawca jest odpowiedzialny względem Zamawiającego za wszelkie wady prawne i fizyczne przedmiotu zamówienia, w tym również za ewentualne roszczenia osób trzecich wynikające z naruszenia praw własności intelektualnej lub przemysłowej, w tym patentów, praw ochronnych na znaki towarowe oraz praw z rejestracji na wzory użytkowe i przemysłowe, pozostające w związku z wprowadzeniem do obrotu na terytorium Rzeczypospolitej Polskiej.

1. Dostawa macierzy do klastra HA - szt. 1

| **LP.** | **Nazwa komponentu** | **Wymagane minimalne parametry techniczne** | **Parametry sprzętu**  **oferowanego przez Wykonawcę** jeżeli asortyment/usługi proponowany przez Wykonawcę posiada parametry takie same jak wskazane przez Zamawiającego wówczas wpisać : **TAK** |
| --- | --- | --- | --- |
|  | **Typ** | **Dostawa macierzy dyskowej do klastra HA** | |
| **Wymagania techniczne wymagania minimalne** | | | |
|  | **Obudowa i komponenty** | System musi być dostarczony ze wszystkimi komponentami do instalacji w szafie rack 19''. Podzespoły macierzy tj. wentylatory, zasilacze muszą być w pełni redundantne. |  |
|  | **Pojemność** | System musi zostać dostarczony w konfiguracji zawierającej minimum:   1. 8 dysków 960GB SSD oraz posiadać możliwość rozbudowy o kolejne dyski. 2. System musi wspierać dyski o wielkościach minimum: od 960GB do 7600GB SSD |  |
|  | **Kontroler** | 1. Dwa kontrolery wyposażone w przynajmniej 32GB cache każdy. 2. W przypadku awarii zasilania dane nie zapisane na dyski, przechowywane w pamięci muszą być zabezpieczone za pomocą podtrzymania bateryjnego przez minimum 72 godziny lub za pomocą zrzutu danych na pamięć nie ulotną. 3. Macierz musi pozwalać na rozbudowę do klastra 24 kontrolerów lub musi pozwalać na obsługę przynajmniej 800 dysków w obrębie pary kontrolerów lub klastra w zależności od sposobu realizacji funkcjonalności. 4. Wszystkie kontrolery muszą pracować pod kontrolą tego samego systemu operacyjnego stworzonego przez producenta urządzenia. Nie dopuszcza się zastosowania systemu, w którym udostępnianiem danych zarządzają różne systemy operacyjne w jednym zintegrowanym urządzeniu. |  |
|  | **Procesor** | Zamawiający wymaga, aby dostarczony system posiadał procesory wykonane w architekturze Intel lub AMD. Dopuszczalne jest zastosowanie procesorów w innej architekturze, przy zachowaniu minimalnej ilości rdzeni 64 na procesor. |  |
|  | **Interfejsy** | Oferowana macierz musi posiadać minimum:   1. 8 portów 10Gb (SFP+) (wymagane dostarczenie minimum 4 wkładek SFP+) 2. 4 porty 10Gb (min. 2 kable typu twinax min. 0,5m) 3. 4 porty 12Gb SAS, 4. 2 porty 1GbE do zarządzania oraz 2 porty konsolowe   Jeśli korzystanie z któregoś z wyżej wymienionych portów wymaga zastosowania wkładek (np. SFP+), zamawiający wymaga ich dostarczenia wraz z urządzeniem. |  |
|  | **RAID** | System RAID musi być skonfigurowany w taki sposób, aby gwarantował dostęp do danych nawet w przypadku jednoczesnej awarii do trzech dysków w jednej grupie RAID. |  |
|  | **Kopie Migawkowe** | Macierz musi być wyposażona w system kopii migawkowych, dostępny dla wszystkich rodzajów danych przechowywanych na macierzy. System kopii migawkowych nie może powodować spadku wydajności macierzy większej niż 5%. |  |
|  | **Obsługiwane protokoły** | Macierz musi obsługiwać jednocześnie protokoły FC; FCoE; iSCSI; NFS; CIFS/SMB oraz S3, z kontrolerów macierzy. Zamawiający w tym postępowaniu wymaga dostarczenia licencji na wszystkie protokoły. |  |
|  | Inne wymagania | 1. Macierz musi posiadać funkcjonalność replikacji danych w trybie asynchronicznym oraz synchronicznym. Funkcjonalność replikacji danych musi być natywnym rozwiązaniem macierzy dyskowej. Przed procesem replikacji macierz musi umożliwiać włączenie procesu deduplikacji danych w celu optymalizacji wykorzystania łącza oraz skrócenia czasu backupu dla replikowanych zasobów. 2. Jeżeli oferowane rozwiązanie nie pozwala na deduplikację replikowanych zasobów zamawiający wymaga dostarczenia zewnętrznego urządzenia do deduplikowania replikowanych danych. W przypadku zastosowania zewnętrznych urządzeń do deduplikacji replikowanych danych, zamawiający wymaga zastosowania ich w formie redundantnej tj. po 2 szt. na macierz. 3. Macierz musi posiadać wsparcie dla systemów: Windows Server, Linux, Oracle Solaris, IBM AIX, HP-UX, macOS, VMware ESX. 4. Macierz musi umożliwiać dynamiczną zmianę rozmiaru wolumenów logicznych bez przerywania pracy macierzy i bez przerywania dostępu do danych znajdujących się na danym wolumenie. 5. Macierz musi posiadać funkcjonalność priorytetyzacji zadań w tym ustawienie max parametrów (I/Ops i Mbps) dla poszczególnych LUN. 6. Macierz musi umożliwiać dynamiczną zmianę rozmiaru wolumenów logicznych bez przerywania pracy macierzy i bez przerywania dostępu do danych znajdujących się na danym wolumenie. 7. Macierz musi posiadać funkcjonalność replikacji danych z inna macierzą tego samego producenta w trybie synchronicznym i asynchronicznym. Funkcjonalność replikacji danych musi być natywnym narzędziem macierzy. Przed procesem replikacji macierz musi umożliwiać włączenie procesu deduplikacji danych i kompresji danych w celu optymalizacji wykorzystania łącza dla replikowanych zasobów lub zamawiający wymaga dostarczenia zewnętrznego narzędzia do deduplikowania replikowanych danych lub dwukrotnego zwiększenia pojemności ze względu na rozważaną w przyszłości replikację całości zasobów. 8. Macierz musi pozwalać na klonowanie danych bez potrzeby fizycznego kopiowania danych na nośnikach. 9. Macierz musi posiadać narzędzie do wykonania spójnego snapshotu dla następujących aplikacji:    1. Vmware    2. SAP    3. Oracle DBMS    4. MS Exchange oraz MS SQL 10. Oferowana konfiguracja macierzy musi pozwalać na osiągnięcie wydajności minimalnie 160 000 IOPS przy 8KB bloku i stosunku 70/30% odczyt/zapis opóźnieniach nie przekraczających 1 ms. Zamawiający wraz z ofertą wymaga dostarczenia oficjalnego dokumentu producenta z wymiarowaniem wydajności oraz dopuszcza możliwość sprawdzenia wydajności macierzy przy odbiorze. 11. Macierz musi posiadać narzędzie umożliwiające generowanie raportu o konfiguracji, utworzonych dyskach logicznych i woluminach oraz ich zajętości wraz z podziałem na rzeczywiste dane, kopie migawkowe oraz dane wewnętrzne macierzy. 12. Macierz musi być wyposażona oprogramowanie do audytu zasobów plikowych w szczególności pozwalać na:     1. blokowanie zapisywania plików z określonym (do zdefiniowania przez administratora) rozszerzeniem     2. monitorowaniu operacji wykonywanych na plikach 13. Z macierzą zamawiający wymaga dostarczenia oprogramowania, które pozwala na:     1. monitoring wykorzystania przestrzeni na macierzy     2. monitoring grup RAIDowych     3. monitoring wykonywanych backupów/replikacji danych między macierzami     4. monitoring wydajności macierzy     5. analizę i diagnozę spadku wydajności 14. Zamawiający dopuszcza zastosowanie oprogramowania zewnętrznego, na pełną max pojemność systemu. 15. Macierz musi posiadać funkcjonalność „Tieringu” zimnych danych na:     1. inną macierz tego samego producenta (z wolnymi dyskami np. NL-SAS)     2. inną macierz dowolnego producenta z protokołem S3 16. Tiering musi być natywnym narzędziem macierzy i wykonywać się automatycznie. 17. Macierz musi posiadać wbudowane lub zewnętrzne narzędzie jako moduł ochrony przed oprogramowaniem typu ransomware, wykorzystujący mechanizmy uczenia maszynowego do analizy aktywności użytkowników oraz operacji systemowych na poziomie zasobów plikowych. Oprogramowanie to musi umożliwiać automatyczne wykrywanie nietypowych lub podejrzanych zachowań (anomalii), które mogą świadczyć o aktywności złośliwego oprogramowania. W przypadku wykrycia potencjalnego ataku ransomware, system musi:     1. automatycznie poinformować administratora o incydencie,     2. zainicjować ochronne kopie migawkowe (snapshots)     3. umożliwiać późniejsze odtworzenie danych do stanu sprzed incydentu. 18. Macierz musi umożliwiać utworzenie wolumenu plikowego z funkcjonalnością WORM (Write Once Read Many), zapewniającą niezmienialność zapisanych danych. Rozwiązanie musi pozwalać na zablokowanie możliwości modyfikacji lub usunięcia plików przez określony przez administratora czas retencji lub na czas nieokreślony (dożywotni). Funkcjonalność ta musi być konfigurowalna na poziomie wolumenu lub pliku i powinna zapewniać zgodność z wymaganiami dotyczącymi archiwizacji i integralności danych. 19. Wszystkie funkcjonalności muszą być dostarczone na maksymalną pojemność urządzenia i pozwalać na wspólne działanie (żadna funkcjonalność nie może wykluczać działania innej funkcjonalności). 20. System przestrzeni dyskowej musi posiadać moduł do audytu zasobów plikowych na wyspecyfikowanym systemie przestrzeni dyskowej pod kątem przechowywanych danych wrażliwych/osobowych. W szczególności moduł musi posiadać:     1. Możliwość przeszukiwania zasobów plikowych na wyspecyfikowanym systemie przestrzeni dyskowej dla środowisk plikowych,     2. system musi pozwalać na utworzenie kategorii przeszukanych plików na:        * nie wrażliwe (ogólne informacje o pracowniku)        * dane osobiste (numer NIP, Pesel)        * dane wrażliwe (dane zdrowotne, informacje o wynagrodzeniu) 21. System musi być zgodny z europejskimi przepisami GDPR (Rodo) w tym móc przeszukiwać i kategoryzować dane po:     1. NIP/Regon     2. Pesel     3. Adresie Email     4. Kontach bankowych |  |
|  | **Gwarancja i serwis** | 1. Okres świadczenia usług serwisowych:   Wykonawca zobowiązany jest do zapewnienia pełnego serwisu gwarancyjnego producenta przez okres minimum 3 lata od dnia dostawy systemu.   1. Czas dostawy części zamiennych:   Części zamienne muszą być dostarczane najpóźniej w następnym dniu roboczym po zgłoszeniu potrzeby ich wymiany przez Zamawiającego lub autoryzowany serwis.   1. Dostęp do centrum serwisowego:   Wykonawca musi zapewnić dostęp do centrum serwisowego producenta 24 godziny na dobę, 7 dni w tygodniu (24/7).   1. Zgłaszanie awarii:   Możliwość zgłaszania awarii musi być dostępna 24/7, zarówno telefonicznie, jak i drogą elektroniczną.   1. Czas reakcji serwisu:   W przypadku awarii krytycznej (np. całkowitej niedostępności systemu), wykonawca zobowiązany jest zapewnić maksymalnie 2 godziny czasu reakcji serwisowej od momentu zgłoszenia.   1. Aktualizacje oprogramowania i dostęp do wiedzy technicznej. Przez cały okres trwania serwisu (minimum 3 lata), Wykonawca musi zapewnić:    1. Dostęp do wszystkich aktualizacji oprogramowania/fimware’u producenta,    2. Dostęp do portalu serwisowego producenta,    3. Dostęp do dokumentacji technicznej, baz wiedzy i materiałów wspierających eksploatację urządzenia. 2. Własność uszkodzonych nośników danych:   W przypadku awarii dysków twardych lub innych nośników danych, uszkodzone komponenty pozostają własnością Zamawiającego i nie podlegają zwrotowi do producenta lub wykonawcy. |  |

1. UPS o mocy 2kVA - szt. 1

| **LP.** | **Nazwa komponentu** | **Wymagane minimalne parametry techniczne** | **Parametry sprzętu**  **oferowanego przez Wykonawcę** jeżeli asortyment/usługi proponowany przez Wykonawcę posiada parametry takie same jak wskazane przez Zamawiającego wówczas wpisać : **TAK** |
| --- | --- | --- | --- |
|  | **Typ** | **Dostawa zasilacza awaryjnego o mocy min. 2kVA** | |
| **Dane techniczne UPS, wymagania minimalne** | | | |
|  | **Technologia** | on-line (VFI), podwójna konwersja |  |
|  | **Moc pozorna** | minimum 2kVA |  |
|  | **Moc rzeczywista** | minimum 2kW |  |
|  | **Sprawność max (dla VFI)** | > 90 % |  |
|  | **Typ obudowy** | rack/tower |  |
|  | **Poziom hałasu** | < 50dB |  |
|  | **Napięcie wejściowe** | 208 V AC / 220 V AC / 230 V AC / 240 V AC |  |
|  | **Zakres napięcia wejściowego** | 80-300 V AC |  |
|  | **Zakres częstotliwości wejściowej** | 40-70 Hz |  |
|  | **Zakres napięcia wyjściowego** | 208 V AC / 220 V AC / 230 V AC / 240 V AC |  |
|  | **Częstotliwość napięcia wyjściowego** | 50 / 60 Hz |  |
|  | **Kształt napięcia wyjściowego** | sinusoidalny |  |
|  | **Czas przełączania sieć – UPS** | 0ms |  |
|  | **Współczynnik odkształceń THDv** | < 5% @ nieliniowe obciążenie |  |
|  | **Przeciążalność w trybie sieciowym** | 100-110% = ostrzeżenie i przejście w bypass po 10 min,  110-130% = ostrzeżenie i przejście w bypass po 1 min,  >130% = przejście w bypass po 3 sek. |  |
|  | **Przeciążalność w trybie bateryjnym** | 100-130% = ostrzeżenie i wyłączenie po 1 min,  >130% = wyłączenie po 3 sek. |  |
|  | **Baterie wewnętrzne w UPS** | minimum 12V; szczelne, bezobsługowe |  |
|  | **Czas podtrzymania (dla 50 % Pmax) - przy zastosowaniu baterii wew.** | minimum 9 min |  |
|  | **Czas ładowania baterii wew w UPS do 90% pojemności** | do 4h |  |
|  | **Możliwość podłączenie zewnętrznych modułów bateryjnych** | wymagane |  |
|  | **Możliwość włączenia testu baterii** | wymagane |  |
|  | **Ilość i typ gniazd wyjściowych** | minimum 6x IEC320 C13 (10 A) |  |
|  | **Zarządzalne gniazda wyjściowe** | wymagane minimum 3 |  |
|  | **Sygnalizacja** | Wyświetlacz LCD, akustyczna |  |
|  | **Test baterii** | wymagana możliwość uruchomienia testu baterii przyciskiem na obudowie zasilacza |  |
|  | **Możliwość pracy w trybie konwertera częstotliwości** | wymagane |  |
|  | **Automatyczne ładowanie po powrocie zasilania** | wymagane |  |
|  | **Automatyczne uruchomienie po powrocie zasilania** | wymagane |  |
|  | **Interfejs komunikacyjny** | RS232, USB HID, SNMP |  |
|  | **Wymagania odnośnie interfejsu sieciowego** | 1. Obsługa protokołu SNMP v3, HTTP/HTTPS, SSH 2. Możliwość zdalnej konfiguracji urządzenia za pośrednictwem portu sieciowego (Ethernet) minimum w zakresie: ustawień sieci LAN, dostępu przez www, telnet, ssh itp., parametrów SNMP v1 i v3, konfiguracji dostępu użytkowników i zmiany haseł 3. Możliwość ustawienia hasła o długości 8 znaków 4. Wsparcie dla LDAP lub RADIUS 5. Możliwość zdalnego odczytania numeru seryjnego urządzenia UPS (SNMP/WWW/SSH) |  |
|  | **Złącze EPO** | wymagane |  |
|  | **Wsporniki do montażu w szafie RACK** | wymagane |  |
|  | **Waga UPS** | do 30kg |  |
|  | **Wymiary UPS** | nie większe niż: wysokość 88mm; szerokość 439mm; głębokość 610mm |  |
|  | **Gwarancja** | minimum 24 miesiące |  |
|  | **Serwis** | 1. Autoryzowany serwis producenta zlokalizowany w Polsce. 2. Naprawa w maksymalnie 5 dni roboczych 3. Serwis realizowany w systemie door to door |  |
|  | **Oprogramowanie** | 1. wsparcie dla systemów: Windows, Linux 2. wymagane wsparcie producenta (telefoniczne oraz mailowe) w języku polskim odnośnie konfiguracji i rozwiązywania problemów. |  |
|  | **Oświadczenia / dokumenty** | 1. certyfikat lub oświadczenie producenta lub wyłącznego dystrybutora o posiadaniu przez oferenta statusu Autoryzowanego Partnera - mającego wiedzę w zakresie doboru i sprzedaży zasilania gwarantowanego (UPS) jeżeli oferent nie jest producentem sprzętu. 2. deklaracja zgodności CE |  |

1. Serwer do pracy w klastrze HA - szt. 2

| **LP.** | **Nazwa komponentu** | **Wymagane minimalne parametry techniczne** | **Parametry sprzętu**  **oferowanego przez Wykonawcę** jeżeli asortyment/usługi proponowany przez Wykonawcę posiada parametry takie same jak wskazane przez Zamawiającego wówczas wpisać : **TAK** |
| --- | --- | --- | --- |
|  | **Typ** | **Serwer typu RACK** | |
| **Wymagania techniczne serwera** | | | |
|  | **Obudowa** | * Do instalacji w szafie Rack 19”, wysokość nie więcej niż 1U, z zestawem szyn do mocowania w szafie i wysuwania do celów serwisowych. |  |
|  | **Procesor** | * Jeden procesor szesnastordzeniowy, przystosowany do pracy ciągłej. * Zaoferowany procesor musi uzyskiwać w teście Passmark CPU Mark, w konfiguracji jednoprocesorowej, wynik min.: 37940 punktów na dzień 20.10.2025 r. – wydruk ze strony internetowej http://www.cpubenchmark.net/ stanowi załącznik nr …… do SWZ (wydruk w wersji .pdf i .png) * Zamawiający nie dopuszcza procesorów o większej ilości rdzeni niż 16 fizycznych z uwagi na optymalizację kosztową licencjonowania aplikacji i systemów operacyjnych, która uzależniona jest od liczby rdzeni procesora. |  |
|  | **Płyta główna** | * Płyta główna dedykowana do pracy w serwerach, wyprodukowana przez producenta serwera z możliwością zainstalowania do dwóch procesorów wykonujących 64-bitowe instrukcje AMD64 lub EM64T (np. AMD Opteron albo Intel Xeon). * Wsparcie dla procesorów do 64 rdzeni o mocy do 385W |  |
|  | **Pamięć operacyjna** | * Zainstalowane minimum 256GB pamięci RAM w kościach po 32GB. * Minimum 16 slotów na pamięć. * Możliwość rozbudowy do 2TB RAM. * Należy dostarczyć najszybszą zalecaną na stronie producenta oferowanego procesora |  |
|  | **Procesor Graficzny** | * Zintegrowana karta graficzna z minimum 16MB pamięci osiągająca rozdzielczość 1920x1200 przy 60 Hz. * 1 port VGA z tyłu serwera |  |
|  | **Dyski/kontroler** | * minimum 2 sztuki dysków SSD M.2 o pojemności min. 480GB z dedykowanym kontrolerem sprzętowym zapewniającym RAID 0 i 1 * backplane dyskowy pozwalający na instalację 8 dysków SAS/SATA/SSD 2.5” * wewnętrzny slot na kartę Micro SD |  |
|  | **Zasilacz** | * Minimum dwa redundantne zasilacze o mocy minimum 750W z certyfikatem minimum Titanium. |  |
|  | **Interfejsy sieciowe** | * Jeden port RJ-45 o przepustowości 1GbE dedykowany dla karty zarządzającej. * Dwie dwuportowe karty 10/25GbE SFP28 wraz z modułami SR obsadzonymi we wszystkich portach. |  |
|  | **Sloty I/O** | * Obudowa z możliwością obsługi do 3 slotów PCIe. W chwili dostawy serwer powinien być wyposażony w minimum dwa sloty PCIe x16 z tyłu obudowy. * Dodatkowy slot na kartę OCP. |  |
|  | **Porty** | * Z przodu obudowy: 1x USB 3.2, 1x USB 2.0 (możliwość lokalnego zarządzania serwerem przez ten port). * Z tyłu obudowy: 3x USB 3.2, 1x VGA. * Wewnątrz obudowy: 1x USB3.2 |  |
|  | **Chłodzenie** | * Redundatne wentylatory N+1 |  |
|  | **Karta Zarządzania** | Niezależna od zainstalowanego na serwerze systemu operacyjnego posiadająca dedykowany port Gigabit Ethernet RJ-45 i zapewniająca:   * zdalny dostęp do graficznego interfejsu Web karty zarządzającej; * zdalny dostęp poprzez SSH do CLI procesora serwisowego * obsługa IPMI 2.0, SNMP v3/v1, CIM-XML, DCMI 1.5, Redfish DMTF * przekierowanie portu szeregowego przez IPMI oraz SSH * zdalne monitorowanie i informowanie o statusie serwera (m.in. prędkości obrotowej wentylatorów, temperatury : Otoczenia, CPU, pamięci DIMM); * Out-of-Band (OOB) monitorowanie obciążenia CPU/Pamięci/IO oraz całego systemu * szyfrowane połączenie (TLS min TLS 1.2) oraz autentykacje i autoryzację użytkownika; * możliwość zamontowania zdalnych wirtualnych napędów, (obrazy ISO) minimum 4 obrazy iso jednocześnie w czasie jednej sesji * możliwość montowania obrazów ISO z lokalnej stacji zarządzającej poprzez przeglądarkę oraz poprzez współdzielone zasoby sieciowe min NFS/CIFS/HTTPS * wirtualną konsolę z dostępem do myszy, klawiatury; * wirtualna konsola oraz montowanie obrazów ISO bez instalacji dodatkowych komponentów Java czy AciveX (musi działać w oparciu o HTML5) * wsparcie dla IPv6; * wsparcie dla; SNMP; IPMI2.0, SSH, Redfish; * możliwość zdalnego monitorowania w czasie rzeczywistym oraz historycznym min 24h poboru mocy oraz temperatur w serwerze; * możliwość zdalnego ustawienia limitu poboru prądu przez konkretny serwer; * integracja z Active Directory * możliwość zdefiniowania min 12 użytkowników lokalnych na karcie zarządzającej * możliwość obsługi zdalnej konsoli przez minimum czterech administratorów jednocześnie; * wsparcie dla dynamic DNS; |  |
|  | **Funkcje zabezpieczeń** | * Hasło włączania, hasło administratora, moduł TPM (wspierający TPM 2.0). Wbudowany czujnik otwarcia obudowy |  |
|  | **Urządzenia hot swap** | * zasilacze, * wentylatory. |  |
|  | **Diagnostyka** | * Możliwość przewidywania awarii dla procesorów, regulatorów napięcia, pamięci, dysków wewnętrznych, wentylatorów, zasilaczy, a także nietypowych temperatur serwera i komponentów wewnętrznych. |  |
|  | **Systemy operacyjne** | Wsparcie dla systemów:   * VMware ESXi 7.0 i 8.0, * SUSE Linux 15 , Redhat Linux (minimum w najnowszej i poprzedniej wersji systemu 8 i 9), Ubuntu 20.04, 22.04, 24.04, * Windows 2019, 2022, 2025 |  |
|  | **Warunki gwarancji** | * 36 miesięcy pełnego wsparcia producenta on-site w trybie NBD oraz pozostawieniem uszkodzonych dysków. * Zamawiający oczekuje zapewnienia możliwości zgłaszania zdarzeń serwisowych w trybie 24x7 następującymi kanałami: telefonicznie, przez Internet oraz z wykorzystaniem aplikacji. * Możliwość sprawdzenia statusu gwarancji poprzez stronę producenta podając unikatowy numer urządzenia oraz pobieranie uaktualnień mikrokodu oraz sterowników. * Zamawiający oczekuje nieodpłatnego udostępnienia narzędzi serwisowych i procesów wsparcia umożliwiających: Wykrywanie usterek sprzętowych z predykcją awarii. * Automatyczną diagnostykę i zdalne otwieranie zgłoszeń serwisowych. * Możliwość rozszerzenia gwarancji przez producenta do 7 lat w trybie 24/7 z gwarantowanym czasem naprawy 6h. * Firma serwisująca musi posiadać ISO 9001:2015 oraz ISO-27001 na świadczenie usług serwisowych oraz posiadać autoryzacje producenta urządzeń – dokumenty potwierdzające należy załączyć do oferty. * Wymagane dołączenie do oferty oświadczenia Producenta potwierdzające, że Serwis urządzeń będzie realizowany bezpośrednio przez Producenta i/lub we współpracy z Autoryzowanym Partnerem Serwisowym Producenta. |  |
|  | **Certyfikaty** | * Serwer musi być wyprodukowany zgodnie z normą ISO-9001:2015, ISO-50001 oraz ISO-14001 * Serwer musi posiadać deklaracja CE. * Oferowany serwer musi znajdować się na liście Windows Server Catalog i posiadać status „Certified for Windows” dla systemów, Microsoft Windows Server 2022, Microsoft Windows Server 2025. |  |

1. Dostawa przełącznika sieciowego szt. 3

| **LP.** | **Nazwa komponentu** | **Wymagane minimalne parametry techniczne** | **Parametry sprzętu**  **oferowanego przez Wykonawcę** jeżeli asortyment/usługi proponowany przez Wykonawcę posiada parametry takie same jak wskazane przez Zamawiającego wówczas wpisać : **TAK** |
| --- | --- | --- | --- |
|  | **Typ** | **Przełącznik sieciowy typu Access 48 port** | |
| **Wymagania funkcjonalne i techniczne** | | | |
|  | **Parametry fizyczne** | 1. Wymiary urządzenia muszą pozwalać na montaż w szafie rack 19", obudowa nie może być wyższa niż 1U. 2. Zasilanie AC 230V. 3. Maksymalny pobór mocy: 60 W. 4. Minimalny zakres temperatury pracy: 0-40ᵒC. |  |
|  | **Interfejsy sieciowe** | Wymaganym jest, aby przełącznik dysponował niezależnymi interfejsami sieciowymi (nie dopuszcza się portów typu combo) w ilości:   1. 48 porty GE RJ-45. 2. 4 porty 10 GE SFP+. |  |
|  | **Zarządzanie** | 1. Wbudowany 1 port konsoli szeregowej do pełnego zarządzania. 2. Zarządzanie przez: command line (w tym poprzez SSH) oraz poprzez graficzny interfejs z wykorzystaniem przeglądarki (HTTPS). 3. Wsparcie dla SNMP w wersjach 1-3 4. Funkcja zarządzania poprzez dedykowany kontroler przełączników lub system zarządzania, pozwalający na automatyczne wykrywanie, centralne konfigurowanie oraz zarządzanie przełącznikami. 5. Funkcja aktualizacji oprogramowania przez TFTP/FTP oraz za pomocą GUI. 6. Konfiguracja w formie pliku tekstowego umożliwiającego edycję konfiguracji offline. 7. Funkcja backupu konfiguracji z poziomu GUI jak również z CLI (TFTP/FTP). 8. Funkcja definiowania administratorów lokalnie oraz wykorzystanie, w tym celu serwerów Radius i TACACS+. 9. Funkcja definiowania ról administratorów z możliwością określenia trybu dostępu (brak, tylko odczyt, odczyt oraz modyfikacja) do wybranych części konfiguracji. 10. Automatycznie wykonywane rewizje konfiguracji |  |
|  | **Parametry wydajnościowe** | 1. Przepustowość urządzenia - min. 176 Gbps (pełna prędkość, tzw. wire-speed na wszystkich portach) oraz min. 260 Mpps. 2. Tablica adresów MAC o pojemności co najmniej 32k wpisów. 3. Opóźnienie wprowadzane przez przełącznik - poniżej 2 mikrosekund. |  |
|  | **Wymagane funkcje** | 1. Funkcja automatycznej negocjacji prędkości i duplexu dla połączeń. 2. Obsługa Jumbo Frames. 3. Obsługa 802.1d (Spanning Tree), 802.1w (Rapid Spanning Tree), 802.1s (Multiple Spanning Tree). 4. Agregacja portów zgodna ze standardem 802.3ad. 5. Obsługa co najmniej 4000 VLAN'ów, zgodna ze standardem 802.1Q. 6. Obsługa routingu statycznego. 7. Port-mirroring. 8. Uwierzytelnianie 802.1x na poziomie portu. 9. Uwierzytelnianie 802.1x w oparciu o adres MAC. 10. W ramach 802.1x wsparcie dla dedykowanego VLAN'u dla gości (guest VLAN). 11. W ramach 802.1x wsparcie dla urządzeń, które nie obsługują tego protokołu, na podstawie adresu MAC urządzenia. 12. W ramach 802.1x wsparcie dla dynamicznego przypisywania VLAN. 13. Obsługa protokołu sFlow. |  |
|  | **Funkcjonalność urządzenia przy integracji z systemem centralnego zarządzania / NAC** | 1. Przełączniki muszą wspierać tryb pracy, w którym są zarządzane przez fizyczny element nadrzędny (przełącznik lub dedykowany kontroler) (tzw. port extender lub element leaf w architekturze spine-leaf). Zakres zarządzania przez element nadrzędny musi zawierać co najmniej:    * Centralne zarządzanie konfiguracją urządzenia    * Aktualizacja oprogramowania realizowana z systemu centralnego zarządzania    * Centralne zarządzanie sieciami VLAN.    * Blokowanie ruchu pomiędzy klientami w ramach jednego VLAN'u    * Rozpoznawanie urządzeń uzyskujących dostęp do sieci, zarówno stacji klienckich, jak i urządzeń typu drukarki, routery, przełączniki, itp.    * Przenoszenie zidentyfikowanych urządzeń do właściwych stref. W przypadku wykrycia urządzenia niepasującego do zaakceptowanych schematów, urządzenie powinno przenieść go do strefy odizolowanej.    * Integrację z systemem kontroli dostępu. Urządzenie musi podejmować decyzje o dostępie na podstawie przynajmniej następujących czynników: nazwy hosta, nazwy użytkownika, typu urządzenia, typu systemu operacyjnego.    * Automatyczna detekcja i rekomendacje konfiguracji.    * Przesyłanie logów na zewnętrzny serwer syslog.    * Funkcja uruchomienia Captive Portalu w celu identyfikacji użytkowników.    * Obsługa białych i czarnych list adresów MAC.    * Wykrywanie aplikacji komunikujących się w sieci. 2. Musi być możliwe redundantne połączenie z elementami zarządzającymi. 3. W ramach postępowania koniecznym jest dostarczenie wszystkich licencji niezbędnych do uruchomienia na przełączniku w/w funkcji, polegających na integracji z systemem centralnego zarządzania lub NAC. |  |
|  | **Funkcje urządzenia przy integracji z systemem centralnego zarządzania** | 1. System musi realizować funkcję Stateful Firewall pomiędzy sieciami VLAN realizowanymi na urządzeniu dostępowym. 2. System musi zapewniać Routing statyczny i dynamiczny (co najmniej OSPF) oraz Policy Based Routing. |  |
|  | **Gwarancja oraz wsparcie** | 1. Gwarancja producenta obowiązująca minimum 24 miesiące, obejmująca naprawę lub wymianę urządzenia w przypadku jego awarii lub wadliwości, z zachowaniem ciągłości działania infrastruktury. 2. Dostarczone urządzenie przełączające musi być objęte wsparciem technicznym producenta do 26.06.2026 r., spełniającym poniższe wymagania:    * dostęp do aktualizacji oprogramowania i poprawek bezpieczeństwa,    * dostępność pomocy technicznej 24 godziny na dobę, 7 dni w tygodniu,    * możliwość zgłaszania usterek przez portal internetowy, e-mail lub telefonicznie,    * przypisanie wsparcia do numeru seryjnego urządzenia, aktywowanego w momencie dostawy. |  |

1. Licencja Windows Serwer wraz z licencjami dostępowymi CAL- kpl. 1

| **LP.** | **Nazwa komponentu** | **Wymagane minimalne parametry techniczne** | **Parametry sprzętu**  **oferowanego przez Wykonawcę** jeżeli asortyment/usługi proponowany przez Wykonawcę posiada parametry takie same jak wskazane przez Zamawiającego wówczas wpisać : **TAK** |
| --- | --- | --- | --- |
|  | **Typ** | **Licencja systemu operacyjnego Windows Server 2025 Standard – 16 Core oraz Licencja dostępowa Windows Server 2025 USER CAL (Client Access License). License w wersji CSP Perpetual. Licencje muszą być dostarczone w modelu CSP Perpetual (Cloud Solution Provider) – licencja wieczysta.**  **Zamówienie obejmuje dostawę kompletnego pakietu licencji serwerowych wraz z niezbędnymi licencjami dostępowymi (CAL), zapewniającego prawidłowe funkcjonowanie środowiska Windows Server w infrastrukturze Zamawiającego. Licencje dostępowe stanowią funkcjonalnie nieodłączny element rozwiązania serwerowego i są niezbędne do realizacji celu zamówienia.**  **W ramach postepowania należy dostarczyć licencje w ilościach:**   * **Windows Server 2025 Standard lub równoważne– 16 Core – 2 szt** * **Windows Server 2025 USER CAL (Client Access License) lub równoważne – 40 szt**   Dopuszcza się zastosowanie rozwiązań równoważnych, pod warunkiem pełnej zgodności funkcjonalnej i technicznej z istniejącym środowiskiem serwerowym Zamawiającego, w szczególności w zakresie:   * kompatybilności z dotychczasowym oprogramowaniem serwerowym, * integracji z usługami Active Directory, politykami grupowymi GPO, * kompatybilności z oprogramowaniem do tworzenia kopii zapasowych Veeam, * możliwości uruchamiania aplikacji wymagających środowiska Windows Server. | |
| **Wymagania funkcjonalne i techniczne** | | | |
|  | **Wymagania dotyczące licencji** | 1. Licencje muszą być w modelu CSP Perpetual (Cloud Solution Provider) – licencja wieczysta. 2. Licencje nie mogą wymagać subskrypcji ani opłat abonamentowych. 3. Licencje muszą być dostarczone w formie elektronicznej. 4. Zamawiający wymaga aby licencje były dostępne poprzez portal Microsoft Admin Center. 5. Licencje muszą umożliwiać uruchomienie systemu operacyjnego Windows Server 2025 Standard w środowisku wirtualnym lub fizycznym, zgodnie z polityką licencyjną Microsoft. |  |
|  | **Warunki realizacji zamówienia** | 1. Wykonawca dostarczy oficjalne potwierdzenie nabycia licencji w formie elektronicznej oraz przypisze licencje do konta Zamawiającego w Microsoft Admin Center. 2. Wykonawca zapewni wsparcie w zakresie aktywacji licencji oraz ich przypisania do konta Zamawiającego. 3. W przypadku problemów z aktywacją lub weryfikacją licencji Wykonawca zobowiązuje się do zapewnienia wsparcia technicznego. |  |
|  | **Wymagania techniczne dla oferowanego rozwiązania (oryginalnego lub równoważnego)** | 1. Licencja musi uprawniać do uruchamiania serwerowego systemu operacyjnego w środowisku fizycznym i dwóch wirtualnych środowiskach serwerowego systemu operacyjnego za pomocą wbudowanych mechanizmów wirtualizacji. 2. Możliwość wykorzystywania 64 procesorów wirtualnych oraz 1 TB pamięci RAM i dysku o pojemności min. 64 TB przez każdy wirtualny serwerowy system operacyjny. 3. 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. 4. Wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany pamięci RAM bez przerywania pracy. 5. Wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany procesorów bez przerywania pracy. 6. Automatyczna weryfikacja cyfrowych sygnatur sterowników w celu sprawdzenia, czy sterownik przeszedł testy jakości przeprowadzone przez producenta systemu operacyjnego. 7. Możliwość dynamicznego obniżania poboru energii przez rdzenie procesorów niewykorzystywane w bieżącej pracy, z uwzględnieniem architektury Hyper Threading. 8. Wbudowany mechanizm klasyfikowania i indeksowania plików (dokumentów) w oparciu o ich zawartość. 9. Wbudowane szyfrowanie dysków przy pomocy mechanizmów posiadających certyfikat FIPS 140-2 lub równoważny wydany przez NIST lub inną agendę rządową zajmującą się bezpieczeństwem informacji. 10. Możliwość uruchamiania aplikacji internetowych wykorzystujących technologię ASP.NET. 11. Możliwość dystrybucji ruchu sieciowego HTTP pomiędzy kilka serwerów. 12. Wbudowana zapora internetowa (firewall) z obsługą definiowanych reguł dla ochrony połączeń internetowych i intranetowych. 13. Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, przeglądarka internetowa, pomoc, komunikaty systemowe. 14. Możliwość zmiany języka interfejsu po zainstalowaniu systemu, dla co najmniej 2 języków poprzez wybór z listy dostępnych lokalizacji. 15. Wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug&Play). 16. Możliwość zdalnej konfiguracji, administrowania oraz aktualizowania systemu. 17. Wsparcie dostępu do zasobu dyskowego SSO poprzez wiele ścieżek (Multipath). 18. Możliwość instalacji poprawek poprzez wgranie ich do obrazu instalacyjnego. 19. Mechanizmy zdalnej administracji oraz mechanizmy (również działające zdalnie) administracji przez skrypty. 20. Możliwość migracji konfiguracji systemu Microsoft Windows Server 2022. 21. Możliwość działania jako kontroler domeny Active Directory oraz pełna kompatybilność z usługami katalogowymi Windows. |  |
|  | **Warunki uznania równoważności** | 1. Za równoważne do wyspecyfikowanego rozwiązania Zamawiający uzna rozwiązanie o tym samym przeznaczeniu, cechach technicznych, jakościowych i funkcjonalnych odpowiadających cechom technicznym, jakościowym i funkcjonalnym wskazanych w opisie przedmiotu zamówienia, lub lepszych, oznaczonych innym znakiem towarowym, patentem lub pochodzeniem. 2. Rozwiązanie równoważne musi pozwalać na zrealizowanie zakładanego przez Zamawiającego celu poprzez parametry wydajnościowe i funkcjonalne, mające wpływ na skuteczność działania, takie same lub lepsze od wskazanych wymagań minimalnych. 3. Użycie w opisie przedmiotu zamówienia nazw rozwiązań służy ustaleniu minimalnego standardu wykonania i określenia właściwości i wymogów technicznych założonych w dokumentacji technicznej dla projektowanych rozwiązań lub też stosowane jest w celu wskazania aktualnie użytkowanego środowiska Zamawiającego, z którym rozwiązanie równoważne powinno być kompatybilne. 4. Wykonawca zobligowany jest do wykazania, że oferowane rozwiązania równoważne spełnią zakładane wymagania minimalne. Wykonawca, który złoży ofertę na produkty równoważne musi do oferty załączyć dokumenty zawierające dokładny opis oferowanych produktów, z którego wynikać będzie zachowanie warunków równoważności. Wykonawca, który posługuje się równoważnymi certyfikatami musi je załączyć do oferty. Przez certyfikat równoważny Zamawiający rozumie certyfikat analogiczny co do zakresu z certyfikatami wskazanymi z nazwy, który potwierdza spełnianie normy charakteryzującej się cechami właściwymi dla normy wymienionej przez Zamawiającego, wystawiony przez niezależny podmiot uprawniony do wystawiania certyfikatów. 5. Brak określenia „minimum” oznacza wymaganie na poziomie minimalnym, a Wykonawca może zaoferować rozwiązanie o lepszych parametrach. 6. W celu zachowania zasad neutralności technologicznej i konkurencyjności dopuszcza się rozwiązania równoważne do wyspecyfikowanych, przy czym za rozwiązanie równoważne uważa się takie rozwiązanie, które pod względem technologii, wydajności i funkcjonalności nie odbiega lub jest lepsze od technologii funkcjonalności i wydajności wyszczególnionych w rozwiązaniu wyspecyfikowanym. 7. Nie podlegają porównaniu cechy rozwiązania właściwe wyłącznie dla rozwiązania wyspecyfikowanego, takie jak: zastrzeżone patenty, własnościowe rozwiązania technologiczne, własnościowe protokoły itp., a jedynie te, które stanowią o istocie całości zakładanych rozwiązań technologicznych i posiadają odniesienie w rozwiązaniu równoważnym. W związku z tym, Wykonawca może zaproponować rozwiązania, które realizują takie same funkcjonalności wyspecyfikowane przez Zamawiającego w inny, niż podany sposób. 8. Przez bardzo zbliżoną (podobną) wartość użytkową rozumie się podobne, z dopuszczeniem nieznacznych różnic nie wpływających w żadnym stopniu na całokształt systemu, zachowanie oraz realizowanie podobnych funkcjonalności w danych warunkach, dla których to warunków rozwiązania te są dedykowane. Rozwiązanie równoważne musi zawierać dokumentację potwierdzającą, że spełnia wymagania funkcjonalne Zamawiającego, w tym wyniki porównań, testów czy możliwości oferowanych przez to rozwiązanie w odniesieniu do rozwiązania wyspecyfikowanego. |  |

1. Oprogramowanie do tworzenia kopii zapasowych maszyn wirtualnych szt. 5

| **LP.** | **Nazwa komponentu** | **Wymagane minimalne parametry techniczne** | **Parametry sprzętu**  **oferowanego przez Wykonawcę** jeżeli asortyment/usługi proponowany przez Wykonawcę posiada parametry takie same jak wskazane przez Zamawiającego wówczas wpisać : **TAK** |
| --- | --- | --- | --- |
|  | **Wymagania ogólne** | 1. Oprogramowanie musi być produktem przeznaczonym do obsługi środowisk DataCenter. Oferowany produkt musi znajdować się w kwadracie liderów Gartner Magic Quadrant for Data Center Backup and Recovery Solutions oraz na ogólnie dostępnej liście referencyjnej Gartner: https://www.gartner.com/reviews/market/data-center-backup-and-recovery-solutions i spełniać minimalne wymaganie : - minimalna liczba referencji 150, - minimalna ocena z referencji 4,5 2. Oprogramowanie musi współpracować z infrastrukturą VMware w wersji 6.x, 7.x i 8.0 oraz Microsoft Hyper-V 2012, 2012R2, 2016, 2019 i 2022. Wszystkie funkcjonalności w specyfikacji muszą być dostępne na wszystkich wspieranych platformach wirtualizacyjnych, chyba, że wyszczególniono inaczej 3. Oprogramowanie musi zapewniać tworzenie kopii zapasowych z sieciowych urządzeń plikowych NAS opartych o SMB, CIFS i/lub NFS oraz bezpośrednio z serwerów plikowych opartych o Windows i Linux. |  |
|  | **Całkowite koszty posiadania** | 1. Oprogramowanie musi być niezależne sprzętowo i umożliwiać wykorzystanie dowolnej platformy serwerowej i dyskowej 2. Oprogramowanie musi tworzyć “samowystarczalne” archiwa do odzyskania których nie wymagana jest osobna baza danych z metadanymi deduplikowanych bloków 3. Oprogramowanie musi mieć mechanizmy deduplikacji i kompresji w celu zmniejszenia wielkości archiwów. Włączenie tych mechanizmów nie może skutkować utratą jakichkolwiek funkcjonalności wymienionych w tej specyfikacji 4. Oprogramowanie nie może przechowywać danych o deduplikacji w centralnej bazie. Utrata bazy danych używanej przez oprogramowanie nie może prowadzić do utraty możliwości odtworzenia backupu. Metadane deduplikacji muszą być przechowywane w plikach backupu. 5. Oprogramowanie musi zapewniać warstwę abstrakcji nad poszczególnymi urządzeniami pamięci masowej, pozwalając utworzyć jedną wirtualną pulę pamięci na kopie zapasowe. Wymagane jest wsparcie dla nieograniczonej liczby pamięci masowych to takiej puli. 6. Oprogramowanie musi pozwalać na tworzenie repozytorium kopii zapasowych bezpośrednio na zasobach Microsoft Azure Blob, Google Cloud Storage, Amazon S3, Wasabi Cloud Storage oraz na innych kompatybilnych z S3 przestrzeniach obiektowych. Dodatkowo, oprogramowanie musi wspierać archiwizowanie tych danych do Microsoft Azure Archive Blob Storage oraz Amazon S3 Glacier. 7. Oprogramowanie musi wspierać niezmienność kopii zapasowych na potrzeby ochrony przed ransomware poprzez niedopuszczenie do usunięcia lub modyfikacji kopii zapasowej w zadanym okresie czasu. 8. Oprogramowanie nie może instalować żadnych stałych agentów wymagających wdrożenia czy upgradowania wewnątrz maszyny wirtualnej dla jakichkolwiek funkcjonalności backupu lub odtwarzania 9. Oprogramowanie musi oferować portal samoobsługowy, umożliwiający odtwarzanie użytkownikom wirtualnych maszyn, obiektów MS Exchange i baz danych MS SQL, Oracle oraz PostgreSQL (w tym odtwarzanie point-in-time) 10. Oprogramowanie musi zapewniać możliwość delegacji uprawnień do odtwarzania na portalu 11. Oprogramowanie musi mieć możliwość integracji z innymi systemami poprzez wbudowane RESTful API 12. Oprogramowanie musi mieć wbudowane mechanizmy backupu konfiguracji w celu prostego odtworzenia systemu po całkowitej reinstalacji 13. Oprogramowanie musi mieć wbudowane mechanizmy szyfrowania zarówno plików z backupami jak i transmisji sieciowej. Włączenie szyfrowania nie może skutkować utratą jakiejkolwiek funkcjonalności wymienionej w tej specyfikacji 14. Oprogramowanie musi posiadać mechanizmy chroniące przed utratą hasła szyfrowania 15. Oprogramowanie musi posiadać architekturę klient/serwer z możliwością instalacji wielu instancji konsoli administracyjnych. 16. Oprogramowanie musi posiadać natywne mechanizmy uwierzytelniania wieloskładnikowego (MFA) w celu dostępu do konsoli administracyjnej |  |
|  | **Wymagania RPO** | 1. Oprogramowanie musi wykorzystywać mechanizmy Change Block Tracking na wszystkich wspieranych platformach wirtualizacyjnych. Mechanizmy muszą być certyfikowane przez dostawcę platformy wirtualizacyjnej 2. Oprogramowanie musi wykorzystywać mechanizmy śledzenia zmienionych plików przy zabezpieczaniu udziałów plikowych. 3. Oprogramowanie musi oferować możliwość sterowania obciążeniem storage'u produkcyjnego tak aby nie przekraczane były skonfigurowane przez administratora backupu poziomy latencji. Funkcjonalność ta musi być dostępna na wszystkich wspieranych platformach wirtualizacyjnych z dokładnością do pojedynczego datastoru 4. Oprogramowanie musi zapewniać tworzenie kopii zapasowych z bezpośrednim wykorzystaniem snapshotów macierzowych. Musi też zapewniać odtwarzanie maszyn wirtualnych z takich snapshotów. Proces wykonania kopii zapasowej nie może wymagać użycia jakichkolwiek hostów tymczasowych. Opisana funkcjonalność powinna działać w środowisku VMware. 5. Oprogramowanie musi posiadać wsparcie dla VMware vSAN potwierdzone odpowiednią certyfikacją VMware. 6. Oprogramowanie musi wspierać kopiowanie backupów oraz zasobów plikowych na taśmy. 7. Oprogramowanie musi mieć możliwość tworzenia retencji GFS (Grandfather-Father-Son) 8. Oprogramowanie musi wspierać bezpośrednią integrację z urządzeniami deduplikacyjnymi. Minimalnie wsparcie wymagane dla Dell DataDomain, HPE StoreOnce, ExaGrid, Fujitsu CS800, Quantum DXi oraz Infinidat InfiniGuard. 9. Oprogramowanie musi wspierać BlockClone API w przypadku użycia Windows Server 2016, 2019 lub 2022 z systemem pliku ReFS jako repozytorium backupu. Podobna funkcjonalność musi być zapewniona dla repozytoriów opartych o linuxowy system plików XFS. 10. Oprogramowanie musi mieć możliwość kopiowania backupów oraz replikacji wirtualnych maszyn z wykorzystaniem wbudowanej akceleracji WAN. 11. Oprogramowanie musi mieć możliwość replikacji asynchronicznej włączonych wirtualnych maszyn bezpośrednio z infrastruktury VMware vSphere pomiędzy hostami ESXi oraz pomiędzy hostami Hyper-V. Dodatkowo oprogramowanie musi mieć możliwość użycia plików kopii zapasowych jako źródła replikacji. 12. Oprogramowanie musi mieć możliwość replikacji ciągłej, opartej o VMware VAIO, włączonych wirtualnych maszyn bezpośrednio z infrastruktury VMware vSphere. Dla replikacji ciągłej musi być możliwość zdefiniowania dziennika pozwalającego na odzyskanie danych z dowolnego punku w ramach ustalonego parametru RPO. 13. Oprogramowanie musi umożliwiać przechowywanie punktów przywracania dla replik 14. Oprogramowanie musi umożliwiać wykorzystanie istniejących w infrastrukturze wirtualnych maszyn jako źródła do dalszej replikacji (replica seeding) 15. Oprogramowanie musi wykorzystywać wszystkie oferowane przez hypervisor tryby transportu (sieć, hot-add, LAN Free-SAN) |  |
|  | **Wymagania RTO** | 1. Oprogramowanie musi umożliwiać jednoczesne uruchomienie wielu maszyn wirtualnych bezpośrednio ze zdeduplikowanego i skompresowanego pliku backupu, z dowolnego punktu przywracania, bez potrzeby kopiowania jej na storage produkcyjny. Funkcjonalność musi być oferowana dla środowisk VMware, Hyper-V oraz Nutanix AHV niezależnie od rodzaju storage’u użytego do przechowywania kopii zapasowych. 2. Dodatkowo dla środowiska vSphere, Hyper-V i Nutanix AHV powyższa funkcjonalność powinna umożliwiać uruchomianie backupu z innych platform (inne wirtualizatory, maszyny fizyczne oraz chmura publiczna) 3. Oprogramowanie musi pozwalać na migrację on-line tak uruchomionych maszyn na storage produkcyjny. Migracja powinna odbywać się mechanizmami wbudowanymi w hypervisor. Jeżeli licencja na hypervisor nie posiada takich funkcjonalności - oprogramowanie musi realizować taką migrację swoimi mechanizmami 4. Oprogramowanie musi pozwalać na zaprezentowanie pojedynczego dysku bezpośrednio z kopii zapasowej do wybranej działającej maszyny wirtualnej vSpehre 5. Oprogramowanie musi pozwalać na uruchomienie zasobów plikowych SMB oraz baz danych MS SQL i Oracle bezpośrednio ze skompresowanego i skompresowanego pliku backupu. Dodatkowo wspierana musi być migracja on-line tak uruchomionych zasobów na środowisko produkcyjne. 6. Oprogramowanie musi umożliwiać pełne odtworzenie wirtualnej maszyny, plików konfiguracji i dysków 7. Oprogramowanie musi umożliwiać pełne odtworzenie wirtualnej maszyny bezpośrednio do Microsoft Azure, Microsoft Azure Stack, Amazon EC2 oraz Google Cloud Platform. 8. Oprogramowanie musi umożliwić odtworzenie plików/folderów lub ich uprawnień na maszynę operatora, lub na serwer produkcyjny bez potrzeby użycia agenta instalowanego wewnątrz wirtualnej maszyny. Funkcjonalność ta nie powinna być ograniczona wielkością i liczbą przywracanych plików 9. Oprogramowanie musi mieć możliwość odtworzenia plików bezpośrednio do maszyny wirtualnej poprzez sieć, przy pomocy natywnego API dla platformy VMware i PowerShell Direct dla platformy Hyper-V. 10. Oprogramowanie musi wspierać odtwarzanie pojedynczych plików z systemów Windows, Linux, BSD, Solaris, Mac, Novell 11. Oprogramowanie musi wspierać przywracanie plików z partycji Linux LVM 12. Oprogramowanie musi umożliwiać szybkie granularne odtwarzanie obiektów aplikacji bez użycia jakiegokolwiek agenta zainstalowanego wewnątrz maszyny wirtualnej. 13. Oprogramowanie musi wspierać granularne odtwarzanie obiektów Active Directory takich jak konta komputerów, konta użytkowników, dowolnych atrybutów, rekordów DNS zintegrowanych z AD, Microsoft System Objects, certyfikatów CA, elementów AD Sites oraz pozwalać na odtworzenie haseł. 14. Oprogramowanie musi wspierać granularne odtwarzanie Microsoft Exchange 2013SP1 i nowszych (dowolny obiekt w tym obiekty w folderze "Permanently Deleted Objects"). Odtwarzanie musi być możliwe bezpośrednio do środowiska produkcyjnego. 15. Oprogramowanie musi wspierać granularne odtwarzanie Microsoft SQL 2008 i nowszych. Odtwarzanie musi być możliwe bezpośrednio do środowiska produkcyjnego dla odzysku point-in-time, całych baz lub pojedynczych tabeli, widoków oraz procedur. 16. Oprogramowanie musi wspierać granularne odtwarzanie Microsoft Sharepoint 2013 i nowszych. Odtwarzanie musi być możliwe bezpośrednio do środowiska produkcyjnego dla odzysku całych witryn, bibliotek oraz pojedynczych dokumentów wraz z historią ich wersji. 17. Oprogramowanie musi wspierać granularne odtwarzanie baz danych Oracle z opcją odtwarzanie point-in-time wraz z włączonym Oracle DataGuard. Funkcjonalność ta musi być dostępna dla baz uruchomionych w środowiskach Windows oraz Linux. 18. Oprogramowanie musi wspierać granularne odtwarzanie baz danych PostgreSQL z opcją odtwarzanie point-in-time. Funkcjonalność ta musi być dostępna dla baz uruchomionych w środowiskach Linux. 19. Oprogramowanie musi posiadać natywną integrację dla backupów wykonywanych poprzez Oracle RMAN 20. Oprogramowanie musi posiadać natywną integrację dla backupów wykonywanych poprzez SAP HANA, SAP Oracle 21. Oprogramowanie musi posiadać natywną integrację dla backupów wykonywanych poprzez MS SQL VDI 22. Oprogramowanie musi wspierać także specyficzne metody odtwarzania w tym "reverse CBT" oraz odtwarzanie z wykorzystaniem sieci SAN |  |
|  | **Ograniczenie ryzyka** | 1. Oprogramowanie musi dawać możliwość stworzenia laboratorium (izolowane środowisko) dla vSphere i Hyper-V używając wirtualnych maszyn uruchamianych bezpośrednio z plików backupu. Powyższa funkcjonalność powinna umożliwiać uruchomianie backupu z innych platform (inne wirtualizatory, maszyny fizyczne oraz chmura publiczna) 2. Dla VMware’a oprogramowanie musi pozwalać na uruchomienie takiego środowiska dla replik maszyn wirtualnych oraz bezpośrednio ze snapshotów macierzowych stworzonych na wspieranych urządzeniach. 3. Oprogramowanie musi umożliwiać weryfikację odtwarzalności wielu wirtualnych maszyn jednocześnie z dowolnego backupu według własnego harmonogramu w izolowanym środowisku. Testy powinny uwzględniać możliwość uruchomienia dowolnego skryptu testującego również aplikację uruchomioną na wirtualnej maszynie. Testy muszą być przeprowadzone bez interakcji z administratorem 4. Oprogramowanie musi umożliwiać integrację z oprogramowaniem antywirusowym w celu wykonania skanu zawartości pliku backupowego przed odtworzeniem jakichkolwiek danych. Integracja musi być zapewniona minimalnie dla Windows Defender, Symantec Protection Engine oraz ESET NOD32. 5. Oprogramowanie musi umożliwiać dwuetapowe, automatyczne, odtwarzanie maszyn wirtualnych z możliwością wstrzyknięcia dowolnego skryptu przed odtworzeniem danych do środowiska produkcyjnego. 6. Licencja wieczysta ze wsparciem do 26.06.2026. |  |

1. Dysk sieciowy NAS - backup szt. 1

|  |  |  |  |
| --- | --- | --- | --- |
| **L.P.** | **Nazwa komponentu** | **Wymagane minimalne parametry techniczne** | **Parametry sprzętu**  **oferowanego przez Wykonawcę** jeżeli asortyment/usługi proponowany przez Wykonawcę posiada parametry takie same jak wskazane przez Zamawiającego wówczas wpisać : **TAK** |
|  | **Typ** | **Serwer NAS w obudowie RACK** | |
|  | **Obudowa** | Rack 19“, 1U, z kompletem szyn do montażu w szafie RACK |  |
|  | **Procesor** | Czterordzeniowy procesor osiągający w teście PassMark na lipiec 2025 co najmniej 5200 punktów |  |
|  | **Sprzętowy mechanizm szyfrowania** | Tak (AES-NI) |  |
|  | **Pamięć RAM** | min. 8 GB pamięci ECC UDIMM z możliwością rozszerzenia do min. 64 GB |  |
|  | **Możliwości rozbudowy** | 1. Sprzęt powinien być wyposażony w min. 4 kieszenie na dyski twarde typu hot-swap z możliwością rozszerzenia do 16 dysków łącznie przy użyciu dodatkowych jednostek rozszerzających podłączanych do jednostki głównej za pomocą gniazda rozszerzeń 2. Wbudowane 2 gniazda M.2 obsługujące dyski SATA/NVMe |  |
|  | **Zainstalowane dyski** | 4 x 8TB HDD |  |
|  | **Porty zewnętrzne** | Minimum:   1. 2 porty USB 3.0 2. 1 gniazdo rozszerzenia |  |
|  | **Porty sieciowe** | Minimum: 4 porty 1GbE RJ45 (z obsługą funkcji Link Aggregation / przełączania awaryjnego) |  |
|  | **Funkcja Wake on LAN/WAN** | Tak |  |
|  | **Gniazdo rozszerzeń PCIe 3.0** | Min. 1x 8-liniowe gniazdo x8 |  |
|  | **Wentylator obudowy** | Min. 2 wentylatory (40 × 40 × 28 mm) |  |
|  | **System plików** | Min.:   1. Wewnętrzny: Btrfs, ext4 2. Zewnętrzny: Btrfs, ext4, ext3, FAT, NTFS, HFS+ |  |
|  | **Obsługiwane typy macierzy RAID** | RAID F1, Podstawowy (basic), JBOD, RAID 0, RAID 1, RAID 5, RAID 6, RAID 10 |  |
|  | **Obsługiwane protokoły sieciowe** | Min. SMB1 (CIFS), SMB2, SMB3, NFSv3, NFSv4, NFSv4.1, NFS Kerberized sessions, iSCSI, HTTP, HTTPs, FTP, SNMP, LDAP, CalDAV |  |
|  | **Zarządzanie pamięcią masową** | 1. Maksymalny rozmiar pojedynczego wolumenu:    * 1 PB (wymagana pamięć 64 GB, tylko grupy RAID 6)    * 200 TB (wymagana pamięć 32 GB)    * 108 TB 2. Minimalna liczba wewnętrznych wolumenów: 256 3. Minimalna liczba obiektów iSCSI Target: 64 |  |
|  | **Obsługiwane protokoły** | SMB1 (CIFS), SMB2, SMB3, NFSv3, NFSv4, NFSv4.1, sesje Kerberized NFS, iSCSI, Fibre Channel, HTTP, HTTPs, FTP, SNMP, LDAP, CalDAV |  |
|  | **Konto i folder współdzielony** | 1. Minimalna liczba kont użytkowników: 2 048 2. Minimalna liczba grup użytkowników: 512 3. Minimalna liczba folderów współdzielonych: 512 |  |
|  | **Usługi plików** | 1. Protokół plików: SMB, AFP, NFS, FTP, WebDAV, Rsync 2. Minimalna liczba jednoczesnych połączeń SMB (oparta na FSCT) z rozszerzeniem RAM: 400 3. Integracja z listą kontroli dostępu Windows (ACL) 4. Uwierzytelnianie Kerberos NFS |  |
|  | **Wirtualizacja** | Obsługa VMware vSphere with VAAI, Windows Server 2022, Citrix, OpenStack. |  |
|  | **Bezpieczeństwo** | Zapora, szyfrowanie folderów współdzielonych, szyfrowanie SMB, FTP przez SSL/TLS, SFTP, rsync przez SSH, automatyczne blokowanie logowania, wsparcie Let's Encrypt, HTTPS (konfigurowalny zestaw szyfrów). |  |
|  | **Oprogramowanie** | 1. Urządzenie musi umożliwiać utworzenie przestrzeni dyskowej w oparciu o nowoczesny system plików, który będzie zapewniał obsługę migawek, generowania sum kontrolnych CRC a także lustrzanych kopii metadanych aby zapewnić całkowitą integralność danych biznesowych. Dodatkowo wspomniany system musi wspierać ustawienie limitu dla folderów współdzielonych oraz szybkie klonowanie całych folderów udostępnionych 2. Urządzenie musi wspierać funkcję WORM (Write Once, Read Many) oraz migawki niezmienne 3. Oprogramowanie zarządzające serwerem NAS musi zapewnić darmowe, kompleksowe rozwiązanie do tworzenia kopii zapasowych przeznaczone dla heterogenicznych środowisk IT, umożliwiające zdalne zarządzanie i monitorowanie ochrony komputerów, serwerów i maszyn wirtualnych na jednym, centralnym, przyjaznym dla administratora interfejsie. Ponadto gromadzone dane na urządzeniu mają mieć możliwość replikacji jako lokalne kopie zapasowe, sieciowe kopie zapasowe i kopie zapasowe danych w chmurach publicznych przy użyciu darmowego narzędzia instalowanego z Centrum Pakietów 4. Wymaga się zapewnienia darmowej aplikacji do realizacji chmury prywatnej bez opłat cyklicznych, która będzie posiadała wygodną konsolę administratora zarządzaną z GUI a także agenty na urządzenia PC/MAC oraz aplikację mobilną na Android/iOS. Usługa powinna umożliwiać udostępnianie zasobów serwera NAS, synchronizację i tworzenie kopii zapasowych podłączonych urządzeń a także wspierać algorytm Intelliversioning. Ponadto omawiana usługa powinna umożliwiać pracę z dokumentami biurowymi (edytor tekstowy, arkusz kalkulacyjny, pokaz slajdów) i wpierać wersjonowanie oraz edycję tworzonych plików office w czasie rzeczywistym. 5. Urządzenie musi umożliwiać pracę w trybie klastra wysokiej dostępności (HA) aby zapewnić nieprzerwany, natychmiastowy dostęp do zasobów bez widocznych zmian w użytkowaniu (konfiguracja jako jeden spójny system).Wszystkie dane z powodzeniem zapisane na serwerze aktywnym będą na bieżąco kopiowane do serwera pasywnego zapewniając replikację w czasie rzeczywistym i dostęp do danych oraz usług w przypadku uszkodzenia jednostki aktywnej dając gwarancję ciągłości pracy. Utworzenie klastra HA ma się opierać o 2 identyczne urządzenia. |  |
|  | **Zasilanie** | Wymogiem jest dostarczenie sprzętu wyposażonego w nadmiarowy zasilacz. |  |
|  | **Gwarancja** | 1. 5 lat na urządzenia główne 2. 1 rok na dodatkowe akcesoria montażowe w postaci przesuwnych szyn rack |  |

1. Mobilne urządzenie do uwierzytelniania dwuskładnikowego szt. 50

| **LP.** | **Nazwa komponentu** | **Wymagane minimalne parametry techniczne** | **Parametry sprzętu**  **oferowanego przez Wykonawcę** jeżeli asortyment/usługi proponowany przez Wykonawcę posiada parametry takie same jak wskazane przez Zamawiającego wówczas wpisać : **TAK** |
| --- | --- | --- | --- |
|  | **Typ** | Mobilne urządzenie do uwierzytelniania dwuskładnikowego, fabrycznie nowe | |
| **Dane techniczne, wymagania minimalne** | | | |
|  | **Rodzaj urządzenia** | Klucz sprzętowy do dwupoziomowego uwierzytelnienia posiadający certyfikację min.: U2F i FIDO2 |  |
|  | **Wsparcie dla platform** | Microsoft Windows, Mac OS, Linux, Chrome OS,; współpraca z mobilnymi systemami operacyjnymi iOS oraz Android |  |
|  | **Kompatybilność z przeglądarkami** | Chrome, Edge, Opera, Safari, Firefox |  |
|  | **Kompatybilność z serwisami** | Google, Microsoft, Twitter, Facebook, Instagram, Gmail, Google Drive i YouTube |  |
|  | **Obowiązkowa interakcja użytkownika podczas logowania** | potwierdzenie logowania dotknięciem przycisku |  |
|  | **Wsparcie dla standardów** | PKCS#11 |  |
|  | **Obsługa algorytmów kryptograficznych** | RSA 2048, RSA 4096 (PGP), ECC p256, ECC p384 |  |
|  | **Klasę szczelności** | Minimum IP67 |  |
|  | **Złącza** | USB A |  |
|  | **Fizyczne właściwości** | Brak baterii; działanie nie wymaga połączenia internetowego do działania; fizycznie skonstruowany, by uniemożliwić jego rozłożenie na części i ponowne złożenie; musi posiadać specjalne oczko umożliwiające zawieszenie urządzenia |  |
|  | **Wymiary** | Max.: 43x24x6 mm |  |
|  | **Dodatkowe wymagania** | Wbudowana karta NFC; |  |
|  | **Zabezpieczenia** | Klucz zabezpieczony przez producenta, by uniemożliwić: wykonania jego kopii na inny klucz lub dokonania manipulacji w obrębie jego oprogramowania |  |
|  | **Oprogramowanie do zarządzania kluczem** | Bezpłatne, możliwe do pobrania ze strony producenta; wymagana dostępność oprogramowania/bibliotek/API na stronie producenta na zasadzie open source, w celu integracji z niestandardowymi aplikacjami; |  |
|  | **Logowanie lub obsługia szyfrowania** | współpraca z min.: smart card, Open PGP, OTP, kody zdarzeniowe i czasowe TOTP/HOTP, statyczne hasło, Challenge-Response |  |
|  | **Gwarancja** | Min. 24 miesiące |  |

1. Dostawa i wdrożenie oprogramowania typu kolektor logów - kpl. 1

| **LP.** | **Nazwa komponentu** | **Wymagane minimalne parametry techniczne** | **Parametry sprzętu**  **oferowanego przez Wykonawcę** (jeżeli asortyment proponowany przez Wykonawcę posiada parametry takie same jak wskazane przez Zamawiającego wówczas wpisać **TAK**) |
| --- | --- | --- | --- |
|  | **Typ** | **Dostawa, instalacja i konfiguracja systemu Centralnego Serwera Logów (CSL) wraz z system wizualizacji zbieranych danych oraz wsparciem** | |
|  | **Oferowany system musi składać się co najmniej z :** | 1. Klaster bazodanowy składający się z co najmniej z 3 węzłów. Węzły klastra mogą być fizycznymi urządzeniami bądź maszynami wirtualnymi. W ramach klastra dane muszą być automatycznie rozproszone pomiędzy węzłami. System musi umożliwiać dodanie do klastra węzła będącego repliką danych. 2. Dashboard - system z interfejsem przeglądarkowym zapewniającym wizualizację danych. Funkcjonalność Dashboard może znajdować się na tym samym urządzeniu fizycznym lub maszynie wirtualnej co Server. 3. Server - dopuszcza się użycie przekaźnika danych zbierającego dane z zewnętrznych systemów, w szczególności wysyłanych poprzez syslog, zarówno po TCP jak i UDP celem późniejszego ich przekazania do centralnej bazy danych. Server musi zapewniać nieprzerwane działanie systemu (klaster min. 2 węzłowy). 4. Celem zapewnienia nieprzerwanego strumienia danych do komponentu Server należy wdrożyć rozwiązanie zapewniające rozkładanie danych (Load Balancer) na podstawie algorytmów min. Round Robin oraz z mechanizmem badania dostępności docelowego systemu Server. 5. Funkcjonalności Dashboard, Server, Load Balancer czy inne niezbędne do działania rozwiązania, nie mogą znajdować się razem z którymkolwiek węzłem klastra bazodanowego. |  |
|  | **System CSL ma zapewniać co najmniej funkcjonalności :** | 1. Zbierania logów (system events) z wspieranych wersji systemów Microsoft Windows Server. 2. Zbierania logów (system events) z wspieranych wersji systemów Microsoft Windows 10 i 11. 3. Agenci na platformę Microsoft Windows muszą mieć możliwość zbierania dowolnie wskazanych logów dowolnych aplikacji pracujących na danym systemie. 4. Zbierania logów z platform Linux o architekturze minimum i386, x86\_64, ARMv7. Agenci zbierający dane muszą być dostępni co najmniej w postaci pakietów deb, rpm, tgz. Musi być zapewniona możliwość dowolnego wskazania zbieranych logów znajdującym się w systemie, w tym logów aplikacji pracujących na danym systemie. Wysyłka logów z systemów Linux może być również realizowana w sposób bezagentowy za pomocą standardu syslog poprzez protokoły TCP i UDP. 5. Autoryzacja agentów mających prawa do wysyłania logów do centralnego systemu musi opierać się o min. jedną z funkcji: interfejs API, hasło, certyfikat. 6. System musi umożliwiać obieranie logów z innych systemów (np. firewall, switch) za pomocą standardu Syslog poprzez protokoły TCP i UDP. 7. System zbierając dane poprzez Syslog musi mieć możliwość identyfikacji źródła poprzez unikalną parę adres IP i port. 8. Dodawanie obsługi kolejnych systemów źródłowych musi odbywać się poprzez system wtyczek, z możliwością tworzenia własnych wtyczek i filtrów. 9. System bazodanowy musi opierać się o rozproszoną bazę NoSQL i oferować funkcjonalność near real-time search. 10. System nie może posiadać wbudowanych limitów licencyjnych na: ilość klastrów, ilość węzłów w klastrze, ilość danych w węźle, ilość danych w klastrze, ilość napływających danych (EPS – events per second). Jedyne ograniczenia mogą wynikać z platformy na której został zainstalowany, tj. ograniczeń platformy wirtualizacyjnej, systemu operacyjnego, fizycznego sprzętu. System przeniesiony na inną, kompatybilną, platformę sprzętową czy programową musi umożliwiać wykorzystanie jej maksymalnych limitów. 11. Dostarczony klaster bazodanowy musi być horyzontalnie skalowany do co najmniej 32 węzłów. 12. Funkcje systemu muszą umożliwiać restart poszczególnych węzłów klastra bez przerywania pracy klastra jako całości i bez utraty napływających danych (tzw. funkcjonalność rolling restart). 13. Baza danych musi umożliwiać automatyczną relokację zbieranych danych pomiędzy węzłami klastra na co najmniej 3 poziomach (np. hot, warm, cold (lub analogiczne)). Relokacja musi być realizowana minimum w oparciu o wiek danych (czas znajdowania się w bazie). 14. System musi umożliwiać automatyczne rotację danych w bazie (indeksie) wg. co najmniej następujących kryteriów: wieku danych (index time), wielkości bazy (index size) oraz ilości wpisów (index message count). 15. System musi umożliwiać wskazanie ilości trzymanych zrotowanych indeksów i automatyczne kasowanie najstarszych indeksów. 16. W ramach dostawy wymagane jest wykonanie pełnej instalacji dostarczanego systemu oraz skonfigurowanie przykładowych integracji z istniejącymi systemami. 17. System musi posiadać funkcjonalność instalacji poprawek bezpieczeństwa rdzenia systemu na bieżąco opisywanych w bazie CVE - Common Vulnerabilities and Exposures (tzw. Kernel LivePatch / HotPatch). Instalacja poprawek musi odbywać się bez konieczności restartu całego systemu. 18. System w przypadku braku odnowienia usług wsparcia nie może zmniejszyć swojej funkcjonalności. Dopuszczalne jest jedynie zaprzestanie działania funkcji "System musi posiadać funkcjonalność instalacji poprawek bezpieczeństwa rdzenia systemu na bieżąco opisywanych w bazie CVE - Common Vulnerabilities and Exposures (tzw. Kernel LivePatch / HotPatch). Instalacja poprawek musi odbywać się bez konieczności restartu całego systemu." |  |
|  | **Wdrożenie** | W ramach usług wdrożeniowych zostanie zainstalowana cała  niezbędna infrastruktura:   1. sprzętowa jeśli dostarczone rozwiązanie ma formę fizycznych urządzeń, 2. wirtualna jeśli dostarczone rozwiązanie ma formę samego  oprogramowania. 3. W przypadku instalacji jako rozwiązanie wirtualne, Zamawiający wskaże 2 fizyczne serwery do instalacji. Wskazane serwery będą bez jakiegokolwiek oprogramowania czy licencji, Oferent musi dostarczyć niezbędną platformę wirtualizacyjną, wraz z  wszystkimi licencjami jeśli wymagane, stosowną do oferowanego  rozwiązania. 4. Należy przeprowadzić instalację oferowanego rozwiązania wraz z integracją z posiadanym rozwiązaniem Firewall, serwerami  Windows/Linux oraz minimum 3 przykładowymi stacjami roboczymi. |  |
|  | **Wsparcie i aktualizacja** | 1. dostęp do dedykowanego systemu HelpDesk, 2. usługa automatycznych aktualizacji krytycznych błędów opisanych w CVE, aktualizacje modułów jądra systemu bez restartu 3. wpięcie w system monitoringu dostępności usług 4. Czas trwania wsparcia do 26.06.2026 |  |

1. Oprogramowanie do zarządzania infrastrukturą IT- 50 użytkowników

|  |  |  |  |
| --- | --- | --- | --- |
| **L.P.** | **Nazwa komponentu** | **Wymagane minimalne parametry techniczne** | **Parametry sprzętu**  **oferowanego przez Wykonawcę** jeżeli asortyment/usługi proponowany przez Wykonawcę posiada parametry takie same jak wskazane przez Zamawiającego wówczas wpisać : **TAK** |
|  | **Typ** | **SYSTEM DO ZARZĄDZANIA INFRASTRUKTURĄ IT** | |
|  | **Architektura / budowa** | 1. System musi umożliwić bezproblemową i stabilną obsługę co najmniej 100 Klientów jednocześnie. 2. Architektura / budowa:    1. Klient – komponent odpowiedzialny za zarządzanie komputerem, zbieranie danych oraz przesyłanie danych do serwera z wykorzystaniem bezpiecznego połączenia, pracujący w trybie usługi systemowej.    2. Konsola administracyjna – przeznaczona do zarządzania całym systemem, w formie w pełni funkcjonalnej aplikacji internetowej (webowej).    3. Panel pracownika – aplikacja webowa, niewymagająca dodatkowego logowania, dostępna dla pracowników, udostępniająca wybrane dane z konsoli administracyjnej oraz pozwalająca na interakcję z pracownikiem w wybranych obszarach.    4. Serwer – oprogramowanie odpowiadające za utrzymywanie komunikacji i wymianę danych z Klientami.    5. Baza danych pracująca na silniku Microsoft SQL Server w wersjach wyspecyfikowanych poniżej. 3. Konfiguracja Architektury:    1. Komponenty systemu (Klient, konsola administracyjna, serwer, baza danych) aktualizują się automatycznie poprzez bezpieczne połączenie.    2. System zawiera mechanizmy automatycznej konserwacji zgodnie z harmonogramem. |  |
|  | **Wymagania systemowe** | 1. Konsola administracyjna musi działać w pełni responsywnie (niezależnie od wielkości i rozdzielczości ekranu urządzenia wyświetlającego) na dowolnej przeglądarce stron WWW zgodnej z HTML5 (np. Internet Explorer 11, FireFox, Chrome, Opera). 2. Klient musi działać na systemach 32 i 64 bitowych: Windows Server 2012/2012R2/2016/2019/2022, Windows 7/8/8.1/10/11, MacOS 10.7/10.8, Linux dla wersji: Ubuntu v.11.04 lub wyższa, Debian v.6.0 lub wyższa, RedHat v.6.0 lub wyższa, CentOS v.6.0 lub wyższa, Fedora v.16 lub wyższa.    1. Klient wspiera poniższe przeglądarki internetowe w zakresie monitorowania aktywności użytkownika w sieci: Opera wersja 63.0.3368.94, Chrome wersja 77.0.3865.90, FireFox wersja 69.0.2 3. Serwer musi działać na systemach 64 bitowych: Windows Server 2016/2019/2022, Windows 7/8/8.1/10/11. 4. Serwer www musi być oparty o platformę Microsoft 64 bit (Windows Server 2016/2019/2022, Windows 10 oraz Java 8 (JRE lub JDK), Apache Tomcat 9. 5. Baza danych musi działać na silniku Microsoft SQL Server 2014/2016/2017/2019/2022 w wersji 64 bitowych bezpłatnej (np. Microsoft SQL Server Express Edition). 6. System musi mieć możliwość pracy w środowisku wirtualnym Microsoft Hyper-V oraz VMWare. |  |
|  | **Interfejsy** | 1. System musi umożliwiać wielokrotny, zgodny z harmonogramem lub na życzenie, import użytkowników, komputerów, struktury organizacyjnej (całości bądź wybranego kontenera) z usługi MS Active Directory, przy czym import struktury organizacyjnej musi następować we wskazane miejsce struktury organizacyjnej zdefiniowanej w systemie. 2. System musi umożliwiać import danych z CSV, Excel, Microsoft SQL Server, MySQL, PostgreSQL 3. System zapewnia integrację z modelem LLM. |  |
|  | **Funkcjonalności systemu zarządzania infrastrukturą IT** | 1. Funkcjonalność Klienta    1. System musi umożliwiać pełne zdalne zarządzanie Klientami, obejmujące uruchamianie i wyłączanie, zmianę konfiguracji Klienta, inicjowanie skanowania oraz wykonanie poleceń systemowych. Klient powinien wyświetlać komunikaty w HTML z dokładnymi danymi o czasie wyświetlenia i użytkowniku. 2. Funkcjonalność konsoli administracyjnej.    1. Konsola administracyjna musi być wielojęzyczna (polski i angielski) i oferować intuicyjny interfejs z pełnym zestawem funkcji zarządzania (dodawanie, modyfikowanie, usuwanie). Musi także zawierać co najmniej 140 różnorodnych dashboardów, w tym dashboardy użytkownika, prezentujące parametry infrastruktury, sieci oraz bezpieczeństwa. Użytkownicy powinni mieć możliwość samodzielnego konfigurowania dashboardów użytkownika, a dashboardy sieciowe i bezpieczeństwa muszą zawierać szczegółowe widżety z informacjami o stanie usług i bezpieczeństwie.    2. W konsoli powinna istnieć funkcja filtrowania danych na dashboardach oraz możliwość personalizacji interfejsu przez użytkownika, w tym definiowanie własnych pól, filtrów i widoków, z zachowaniem tych ustawień pomiędzy sesjami. Konsola musi także umożliwiać definiowanie poziomów uprawnień dla użytkowników i grup, z opcją dziedziczenia oraz integrację z Active Directory dla zarządzania dostępem.    3. Konsola powinna posiadać zaawansowane funkcje zarządzania rekordami, w tym wykonanie poleceń na wielu rekordach jednocześnie oraz dostęp do szczegółowych informacji o pracy urządzeń. 3. Funkcjonalność panelu pracownika    1. Panel pracownika systemu musi automatycznie uruchamiać się i autoryzować przy logowaniu użytkownika, z możliwością definiowania zakresu dostępnych informacji przez administratora dla poszczególnych grup pracowników. Panel kierownika powinien dodatkowo agregować i analizować dane z paneli pracowników. Informacje w panelu muszą być organizowane w logiczne sekcje, które można indywidualnie lub grupowo włączać i wyłączać przez administratora. 4. Zarządzanie licencjami    1. System musi umożliwiać kompleksowe zarządzanie licencjami w różnych modelach i strukturach organizacyjnych, w tym audyty, zarządzanie oprogramowaniem i oprogramowaniem zabronionym, oraz przypisywanie i rozliczanie różnych typów licencji. Musi także rejestrować historię licencji oraz zapewniać funkcje inwentaryzacji i zdalnej dezinstalacji oprogramowania. 5. Wzorce aplikacji i pakietów    1. System powinien posiadać rozbudowaną bazę wzorców oprogramowania, umożliwiać definiowanie własnych wzorców i automatycznie importować nowe wzorce od producenta. Musi także dostarczać szczegółowe informacje o zainstalowanych pakietach i ich wykorzystaniu, w tym edycje Microsoft Office. 6. Inwentaryzacja sprzętu komputerowego i urządzeń.    1. System musi oferować rozbudowane funkcje inwentaryzacji sprzętu komputerowego, włączając automatyczną inwentaryzację zarówno w sieci lokalnej jak i zdalnej, szczegółowe skanowanie komponentów (np. RAM, monitory, dyski twarde) oraz zarządzanie informacjami o zainstalowanym sprzęcie. Powinien także umożliwiać ewidencję zmian konfiguracji sprzętu, identyfikować i klasyfikować urządzenia podłączane do komputerów oraz monitorować historię ich podłączeń. 7. Inwentaryzacja urządzeń sieciowych.    1. System musi posiadać zdolności do identyfikacji i zarządzania środowiskami wirtualizacji Hyper-V i VMware oraz urządzeniami sieciowymi. Wymagane jest posiadanie skanera sieci i SNMP oraz dla środowisk wirtualizacji, które automatycznie zbierają dane, analizują jakość połączeń i identyfikują urządzenia na sieci. System powinien także umożliwiać zdalną instalację Klientów i generowanie map sieci. 8. Inwentaryzacja sprzętu.    1. System musi umożliwiać wszechstronną inwentaryzację sprzętu, włączając urządzenia inne niż komputery (np. drukarki, routery). Musi zapewniać zarządzanie dokumentacją związaną z urządzeniami, monitorować ich ruch oraz przypominać o terminach gwarancji i umowach utrzymaniowych. 9. Ochrona danych (DLP)    1. Ochrona danych (DLP) musi obejmować automatyczne tworzenie listy podłączanych do komputerów urządzeń USB i ich klasyfikację. System powinien dostarczać informacje o historii użytkowania urządzeń zewnętrznych oraz umożliwiać zarządzanie dozwolonymi do użytku urządzeniami USB zgodnie z zdefiniowanymi regułami. 10. Szyfrowanie dysków wewnętrznych oraz zewnętrznych     1. System musi obsługiwać kompleksowe szyfrowanie dysków wewnętrznych i zewnętrznych USB, z wykorzystaniem BitLocker i różnych metod szyfrowania, takich jak XTS\_AES\_256 i AES\_128. Musi umożliwiać zdalne zarządzanie procesem szyfrowania/deszyfrowania, w tym masowe operacje na partycjach systemowych i niesystemowych, zarówno lokalnie, jak i zdalnie (poza NATem). Klucze szyfrujące są przechowywane i chronione w konsoli administracyjnej, dostępne tylko po uwierzytelnieniu administratora. Proces szyfrowania odbywa się w sposób niewidoczny dla użytkownika i nie może być przez niego przerwany, z wyjątkiem stanów hibernacji i wyłączenia systemu, po których jest automatycznie kontynuowany. 11. Zdalna administracja komputerami     1. System musi oferować kompleksową zdalną administrację komputerami, włączając w to automatyczne wykonywanie dowolnych poleceń (np. zarządzanie aplikacjami, plikami, rejestrami systemowymi) oraz zarządzanie cyklicznymi zadaniami z harmonogramem. Powinien obsługiwać technologię Intel vPro dla zdalnej konfiguracji i zarządzania, a także pozwalać na zdalne przejęcie kontroli nad komputerem za pomocą technologii Ultra VNC, umożliwiając operowanie na wielu sesjach jednocześnie. System powinien integrować zaawansowane mechanizmy skryptowe wspierane przez AI dla automatycznego generowania poleceń oraz umożliwiać zarządzanie i tworzenie zadań cyklicznych z różnorodnymi opcjami cykliczności i zakończenia. 12. System musi umożliwiać zdalne w technologii WEBRTC.     1. System musi zapewniać zdalne zarządzanie komputerami przy użyciu technologii WEBRTC, umożliwiając jednoczesne połączenia z wieloma urządzeniami. Powinien oferować funkcje takie jak przejęcie kontroli nad pulpitami, zarządzanie plikami, uruchamianie i zarządzanie aplikacjami oraz instalowanie oprogramowania i aktualizacji. System powinien umożliwiać konfigurację połączeń WEBRTC, w tym instalację i konfigurację odpowiednich serwerów i portów. Dodatkowo, system powinien obsługiwać różne tryby przejęcia sesji, włączając opcje z lub bez zgody użytkownika, a także umożliwiać nagrywanie i zarządzanie sesjami połączeń, w tym wykonywanie zrzutów ekranu i nagrywanie sesji. System powinien również wspierać różnorodne konfiguracje wyświetlania i jakości sesji, a także umożliwiać uruchomienie do 12 sesji na jednym ekranie. 13. System musi zezwalać na wykonywanie zapytań WMI bez zdalnego połączenia do urządzenia. 14. System musi zezwalać na edycję rejestrów urządzenia bez wykorzystania zdalnego połączenia pulpitu. 15. Zdalna instalacja     1. System musi umożliwiać zdalną instalację pakietów MSI i plików .exe, korzystając z Windows Management Instrumentation (WMI) oraz usługi Klient bez dodatkowych poświadczeń, wykorzystując lokalne i sieciowe repozytoria. Powinien obsługiwać tworzenie repozytorium instalatorów z możliwością dodawania aplikacji, zarządzania wersjami oraz kategoryzacji. System musi również umożliwiać tworzenie grup instalacyjnych, definiowanie schematów instalacyjnych i automatyzację procesu instalacji na nowych urządzeniach. Powinien zawierać kiosk aplikacji umożliwiający użytkownikom samodzielną instalację aplikacji oraz rejestrować i raportować wszystkie procesy instalacji, umożliwiając również ich przerwanie. 16. Zarządzanie Poprawkami i Aktualizacjami     1. System musi zapewniać ciągłe monitorowanie i identyfikację brakujących aktualizacji systemowych i komponentów infrastruktury IT, oferując funkcje rozpoznawania niezainstalowanych poprawek, ich pobierania, oraz klasyfikacji. Musi umożliwiać aktualizacje bez zakłócania pracy użytkowników, zarówno zbiorowo jak i indywidualnie, z opcją szybkiego przywrócenia poprzedniego stanu systemu poprzez odinstalowanie niechcianych poprawek. System powinien również umożliwiać pomijanie niechcianych poprawek i dostarczać szczegółowe raporty dotyczące stanu aktualizacji oraz urządzeń, które mogą wymagać restartu. 17. Zdalne Zarządzanie Zaporą (Firewall)     1. System musi umożliwiać zdalne zarządzanie zaporą sieciową (firewall) globalnie w infrastrukturze, co obejmuje monitorowanie jej stanu w czasie rzeczywistym, definiowanie złożonych zasad zapory z centralnego panelu administracyjnego oraz szybkie identyfikowanie i reagowanie na potencjalne zagrożenia sieciowe. 18. Automatyzacja     1. System musi oferować możliwość ustalania harmonogramu dla czynności konserwacyjnych, naprawczych i porządkujących, z opcją ustalania częstotliwości i parametrów wejściowych dla każdej czynności oraz możliwością ich zatrzymania lub uruchomienia. Dodatkowo, system musi posiadać mechanizmy automatyzacji takie jak wykonywanie kopii bezpieczeństwa, identyfikacja aplikacji i pakietów, porządkowanie bazy danych oraz usuwanie nadmiarowych danych. System również powinien wysyłać alerty o zdarzeniach takich jak nowe komputery w bazie danych, braki w licencjach i inne zdarzenia krytyczne dla infrastruktury IT. 19. Zarządzanie magazynem IT     1. System musi umożliwiać efektywne zarządzanie magazynem IT, włączając obsługę dowolnej ilości magazynów w różnych lokalizacjach oraz obsługę dokumentów magazynowych typu PZ, RW, WZ, i inne. System powinien prowadzić ewidencję materiałów w magazynach zgodnie z metodą FIFO. Ponadto, system powinien umożliwiać automatyczne łączenie dokumentów magazynowych z zasobami systemu oraz zapewniać przegląd wszystkich dokumentów. 20. Repozytorium     1. Konsola administracyjna systemu musi być wyposażona w repozytorium dokumentów dowolnego typu, które umożliwia dodawanie nowych dokumentów, przeszukiwanie. Repozytorium powinno także umożliwiać definiowanie kontenerów na dokumenty, co ułatwia organizację i zarządzanie dokumentacją. 21. Kody kreskowe     1. System musi wspierać obsługę kodów kreskowych jedno i dwuwymiarowych, umożliwiając parametryzację kodu pod względem wielkości i atrybutów graficznych. System powinien umożliwiać podgląd oraz wydruk kodów kreskowych. 22. Wysyłanie wiadomości     1. System musi oferować funkcję komunikatora, umożliwiającą bezpośrednią wymianę wiadomości między użytkownikami a administratorem systemu, w tym inicjowanie czatu przez administratora oraz przechowywanie historii konwersacji. System powinien także umożliwiać wysyłanie jednorazowych wiadomości ALERT oraz tworzenie szablonów wiadomości do regularnego użytku, z opcją konfiguracji terminu, po którym wiadomość wygaśnie. Ponadto, system powinien wspierać szkolenie pracowników za pomocą wiadomości tekstowych z możliwością definiowania treści szkoleniowych i automatycznego ich wysyłania. 23. System musi posiadać możliwość eksportu / importu treści. 24. Monitorowanie drukarek sieciowych i wydruków     1. System musi umożliwić monitorowanie i zarządzanie wydrukami z dowolnej drukarki (lokalnej czy sieciowej), rejestrując szczegółowe informacje o każdym wydruku, w tym koszty, dzięki wbudowanemu cennikowi. System powinien również prognozować przyszłe koszty drukowania oraz pozwalać na zarządzanie drukarkami według różnych parametrów, w tym statusu i materiałów eksploatacyjnych. 25. Monitorowanie stron www     1. System musi oferować monitorowanie aktywności internetowej użytkowników na różnych przeglądarkach, nawet przy szyfrowanych połączeniach (https), rejestrując detale takie jak adresy IP, czas połączenia, a także analizując treści stron za pomocą algorytmów sztucznej inteligencji do klasyfikacji i kontroli treści. 26. Monitorowanie serwerów WWW     1. System musi zapewniać monitorowanie wybranych serwerów WWW, prezentując informacje o ich statusie i aktywności, umożliwiając analizę treści stron oraz graficzną prezentację danych związanych z ich działaniem, w tym czasem odpowiedzi i aktywnością w określonym okresie. 27. Monitorowanie dziennika zdarzeń     1. System musi posiadać zdolność do monitorowania dziennika zdarzeń komputerów, umożliwiając definiowanie i filtrowanie zdarzeń według różnych kategorii. 28. System musi umożliwiać monitorowanie komunikatów Syslog. 29. Monitorowanie pracy komputerów     1. System musi oferować monitorowanie pracy komputerów, w tym dat startu i zakończenia pracy, logowania użytkowników, a także zdalne monitorowanie sesji połączeń, rejestrując szczegóły takie jak adresy IP i dane użytkowników. 30. Monitorowanie uprawnień ACL     1. System musi umożliwić skanowanie i monitorowanie uprawnień ACL, oferując szczegółowe raporty, automatyczną aktualizacją danych i filtrami do zarządzania informacjami. 31. Monitorowanie sensorów     1. System musi integrować monitoring warunków środowiskowych za pomocą sensorów po SNMP, umożliwiając graficzną prezentację danych, wysyłanie alertów. 32. Repozytorium CMDB     1. System musi posiadać zintegrowane repozytorium CMDB, umożliwiające zarządzanie zasobami IT, w tym szczegółowe informacje o użytkownikach, urządzeniach, licencjach, a także o oprogramowaniu i jego licencjach, z możliwością importu i eksportu danych. 33. Worktime manager     1. System musi umożliwiać monitorowanie i analizę czasu pracy użytkowników, z możliwością definiowania grup przypisanych do przełożonych i prezentacji szczegółowych danych o aktywności użytkowników w formie widżetów i danych analitycznych. Informacje o czasie pracy, sesjach, aktywności w aplikacjach oraz produktywności powinny być możliwe do udostepnienia w panelu pracownika. 34. Raportowanie i eksport danych     1. System musi oferować zaawansowane możliwości raportowania i eksportu danych, umożliwiając wyeksportowanie informacji do różnych formatów, w tym xls, csv, html, oraz graficznych. Powinien także wspierać generowanie wieloparametrycznych raportów z możliwością stosowania filtrów, obsługę wieloinstancyjności raportowania oraz integrację z narzędziami do tworzenia raportów takimi jak SAP Crystal Reports i Stimulsoft, obejmując co najmniej 150 zdefiniowanych raportów. Dodatkowo, system musi posiadać możliwość konfiguracji harmonogramu umożliwiającego cykliczne wysyłanie raportów oraz zapisywanie ich w dowolnym miejscu, z automatycznym generowaniem raportu w formacie PDF jako wynikiem wykonania harmonogramu. 35. System musi zapewnić interfejs API.     1. System musi oferować rozbudowany interfejs API, umożliwiający komunikację za pomocą REST API. Musi on zapewniać szyfrowaną komunikację z użyciem protokołu TLS 1.3 oraz możliwość tworzenia złożonych requestów JSON. Klucze zabezpieczeń powinny być modyfikowalne i mogą mieć co najmniej 32 znaki. 36. Powiadomienia     1. System musi umożliwiać generowanie różnorodnych powiadomień, w tym alertów w konsoli, e-maili oraz wiadomości SMS, z możliwością edycji treści powiadomień i definiowania grup odbiorców. Powinien obsługiwać automatyczne wywoływanie zadań i integrować się z CMD oraz Windows PowerShell, zapewniając co najmniej 30 predefiniowanych powiadomień oraz możliwość ich personalizacji. 37. Bezpieczeństwo     1. System musi zapewniać rozbudowane funkcje bezpieczeństwa, w tym definicję i zarządzanie prawami dostępu oraz zaawansowane opcje uwierzytelniania. Wymaga silnych haseł, obsługuje wieloskładnikowe uwierzytelnianie i posiada mechanizmy szyfrowania danych. 38. Wsparcie i pomoc     1. Pomoc techniczna     2. Musi być świadczona co najmniej w dni robocze w godzinach od 8.00-16.00.     3. Utrzymaniem Oprogramowania jest zapewnienie aktualizacji Oprogramowania (asysta techniczna) oraz nieprzerwanego działania Oprogramowania (usługi SLA), jak również zapewnienie świadczenia innych usług wspomagających korzystanie z Oprogramowania. |  |
|  | **Wsparcie** | Czas trwania usługi SLA wynosi minimum do 26.06.2026 r., |  |

1. Prace wdrożeniowe sieci LAN i klastra HA - usługa kpl.1

**A. Zakres prac wdrożeniowych – infrastruktura sieciowa LAN**

**A.1 Instalacja i konfiguracja przełączników sieciowych**

* Montaż przełączników sieciowych w szafach RACK, zgodnie z zatwierdzonym schematem połączeń.
* Wykonanie połączeń między przełącznikami a urządzeniami serwerowymi i macierzą.
* Konfiguracja podstawowa urządzeń sieciowych, w tym:
  + konfiguracja portów typu access i trunk,
  + zabezpieczenia warstwy 2 (STP, Port Security, Storm Control).
* Weryfikacja poprawności połączeń i przepustowości na poziomie 10 Gb/s.

**B. Zakres prac wdrożeniowych – środowisko serwerowe i usługi**

**B.1 Instalacja i konfiguracja środowiska serwerowego wysokiej dostępności (HA)**

* Montaż dwóch serwerów w szafie RACK.
* Instalacja i konfiguracja systemu wirtualizacji (zgodnie z ustaleniami z Zamawiającym).
* Utworzenie klastra wysokiej dostępności (HA) z wspólną przestrzenią danych.
* Integracja klastra z zewnętrznym systemem pamięci masowej.
* Włączenie mechanizmów replikacji i automatycznego przełączania (failover).
* Test poprawności działania klastra i czasów przełączenia usług.

**B.2 Wdrożenie kontrolera domeny i usług katalogowych**

* Instalacja i konfiguracja kontrolera domeny Active Directory (AD) w środowisku serwerowym.
* Migracja kont użytkowników, grup, zasad GPO, DNS i struktur OU z dotychczasowego środowiska.
* Test poprawności logowania i replikacji w domenie.
* Opracowanie dokumentacji konfiguracji AD i zasad bezpieczeństwa.

**B.3 Migracja środowiska produkcyjnego**

* Migracja maszyn wirtualnych, usług oraz danych z dotychczasowego środowiska serwerowego do nowej infrastruktury.
* Uruchomienie i testy usług produkcyjnych (m.in. AD, DNS, DHCP, serwery plików, bazy danych).
* Weryfikacja zgodności i integracji z aktualnym systemem użytkowników.

**B.4 Konfiguracja i uruchomienie systemu tworzenia kopii zapasowych**

* Instalacja i konfiguracja oprogramowania do backupów wirtualnych środowisk serwerowych.
* Utworzenie repozytoriów kopii zapasowych (lokalnych i zdalnych).
* Definicja polityki retencji, rotacji i częstotliwości kopii zapasowych (np. zgodnie z zasadą 3-2-1).
* Wykonanie testów odtworzeniowych w celu potwierdzenia integralności danych.

**B.5 Konfiguracja repozytoriów danych i pamięci masowych**

* Konfiguracja centralnego systemu pamięci masowej dla środowiska serwerowego.
* Utworzenie udziałów sieciowych lub wolumenów w protokole iSCSI / NFS / SMB w zależności od potrzeb.
* Konfiguracja systemu sieciowego do kopii zapasowych i archiwizacji danych.
* Wdrożenie procedury synchronizacji lub replikacji danych pomiędzy lokalizacjami.

**B.6 Testy, dokumentacja i szkolenie administratora**

* Przeprowadzenie testów wydajnościowych i stabilności środowiska (klaster, backup, macierz, sieć).
* Wykonanie dokumentacji powykonawczej obejmującej:
  + konfigurację środowiska wirtualnego,
  + ustawienia backupu i repozytoriów danych,
  + politykę bezpieczeństwa i rotacji kopii zapasowych.
* Przekazanie kopii konfiguracji urządzeń (sieciowych, serwerowych, pamięci masowych, UPS).
* Szkolenie podstawowe administratora systemu w zakresie obsługi środowiska wirtualnego, backupów i zarządzania danymi.

**B.7 Koordynacja i odbiór końcowy**

* Opracowanie planu wdrożenia z harmonogramem etapów.
* Wykonanie odbiorów częściowych po zakończeniu każdego etapu.
* Test końcowy potwierdzający działanie środowiska oraz przekazanie pełnej dokumentacji powykonawczej.

Wykonawca zobowiązany jest do dostarczenia niezbędnych materiałów instalacyjnych, w tym:

* wkładek światłowodowych typu SFP+ lub równoważnych, umożliwiających transmisję z prędkością co najmniej 10 Gb/s,
* patchcordów światłowodowych zakończonych złączami LC/LC, w standardzie OM3 lub wyższym,
* kabli połączeniowych i akcesoriów montażowych niezbędnych do wykonania połączeń między przełącznikami sieciowymi, serwerami oraz systemem pamięci masowej.

Dokładna liczba i długości połączeń zostaną uzgodnione z Zamawiającym przed rozpoczęciem prac wdrożeniowych, w oparciu o ostateczny schemat połączeń logicznych i fizycznych zatwierdzony przez Zamawiającego.

1. Aplikacja wspierająca utrzymanie SZBI
2. **Przedmiot zamówienia**

Przedmiot zamówienia obejmuje zakup i dostawę 1 szt. specjalistycznego systemu - oprogramowania wspomagającego systemowe zarządzanie urzędem w zakresie bezpieczeństwa informacji.

1. **Wymagania ogólne oprogramowania**
2. Oprogramowanie ma być dostarczone w najnowszej wersji w języku polskim.
3. Oprogramowanie powinno posiadać dokumentację użytkownika opisującą funkcjonalność każdego z modułów oprogramowania oraz dokumentację administratora opisującą sposób administrowania programem w tym jego instalowania, konfiguracji, sposobu tworzenia kopii zapasowych oraz odtwarzania w przypadku awarii,
4. Program powinien umożliwiać pracę zarówno na komputerach stacjonarnych jak i na urządzeniach mobilnych np. smartfonach.
5. Program na komputerze klienckim powinien posiadać możliwość instalacji jako aplikacja PWA.
6. Koszt zakupu oprogramowania powinien uwzględniać koszt wszystkich składników oprogramowania (poza systemem operacyjnym zainstalowanym na serwerze Zamawiającego), które są niezbędne do jego pracy zgodnie z niniejszą specyfikacją.
7. W ramach zamówienia Zamawiający otrzyma wersję instalacyjną oprogramowania oraz licencję uprawniającą do korzystania z przedmiotowego oprogramowania.
8. Dostawca przez okres jednego roku licząc od dnia przekazania oprogramowania zapewnia wsparcie, w ramach którego Zamawiający zostanie uprawniony do nieodpłatnego pobierania poprawek i aktualizacji oraz na bieżąco pomocy (nadzoru) w obsłudze programu.
9. **Techniczne dane oprogramowania**
10. Program powinien pracować jako aplikacja intranetowa uruchamiana i prawidłowo pracująca w aktualnych wersjach przeglądarek internetowych (MS Edge, Google Chrome, FireFox).
11. Wszystkie dane gromadzone w oprogramowaniu powinny być zapisywane wyłącznie centralnie, na komputerze pełniącym rolę serwera pracującego w trybie ciągłym przez 24 godziny na dobę.
12. Serwer będzie dostarczony przez Zamawiającego i będzie znajdował się w jego siedzibie.
13. Program powinien pracować na serwerze z procesorem 8-rdzeniowy w architekturze

64 bit., min. 1TB SSD, min. 16GB RAM z zainstalowanym systemem operacyjny Windows lub Linux (inne składniki oprogramowania niezbędne do pracy programu dostarcza Dostawca).

1. Aplikacja instalowana na serwerze działającym w systemie Windows powinna posiadać automatyczny instalator wszystkich składników niezbędnych do prawidłowego działania oprogramowania.
2. Poza instalatorem dla systemu Windows aplikacja powinna mieć możliwość uruchomienia na serwerze pracującym pod systemem Linux (konfiguracja instalacji niestandardowych powinna być określona w dokumentacji programu).
3. Program ma mieć możliwość importu użytkowników z przygotowanego zgodnie ze specyfikacją pliku lub ich importu bezpośrednio z Active Directory.
4. Program ma mieć możliwość opcjonalnej integracji z Active Directory.
5. **Funkcjonalność oprogramowania i jego zakres działania**
6. Specjalistyczne oprogramowanie do zarządzania urzędem w zakresie m.in. bezpieczeństwa informacji i ochrony danych osobowych musi posiadać funkcjonalności, które umożliwiają zarządzanie obszarami m.in.:
7. procesami realizowanymi w urzędzie – w tym zakresie oprogramowanie musi:

* posiadać rejestr zidentyfikowanych procesów w tym procesów z zakresu ochrony danych, który umożliwia ich podział na makroprocesy,
* posiadać możliwość opisu procesu poprzez określenie początku i końca procesu, danych wejściowych i wyjściowych procesu, dostawcę, klienta procesu, zakresu podmiotowego i przedmiotowego, dokumentów wymaganych w procesie oraz ryzyk wpływających na osiąganie celu procesów,
* posiadać graficzny edytor do tworzenia interaktywnych map procesów (z możliwością podpinania plików pod dowolne elementy grafu),

1. komórkami organizacyjnymi – w tym zakresie oprogramowanie musi:

* posiadać rejestr komórek organizacyjnych, który będzie oparty na zatwierdzonym w Urzędzie regulaminie organizacyjnym,
* posiadać możliwość opisu komórki organizacyjnej poprzez określenie jej podrzędności w strukturze organizacyjnej, przypisania do niej stanowisk pracy oraz zakresu zadań jaki realizuje,

1. stanowiskami pracy – w tym zakresie oprogramowanie musi:

* posiadać rejestr stanowisk pracy przypisanych do właściwych komórek organizacyjnych, zgodnie z obowiązującym regulaminem organizacyjnym,
* posiadać możliwość opisania stanowiska pracy poprzez określenie m.in.: miejsca stanowiska pracy w strukturze organizacyjnej, celu istnienia stanowiska pracy, liczby podległych pracowników, głównych zadań realizowanych na stanowisku pracy, wymaganych upoważnień i pełnomocnictw obowiązujących na danym stanowisku pracy oraz wymaganiach w zakresie kompetencji czy doświadczenia,

1. pracownikami – w tym zakresie oprogramowanie musi:

* posiadać rejestr wszystkich pracowników, praktykantów i stażystów oraz osób świadczących pracę na umowach cywilnoprawnych,
* posiadać możliwość prześledzenia historii zatrudnienia pracownika, w zakresie m.in. obejmowanych stanowisk pracy, pełnionych przez niego funkcji i posiadanych uprawnień w aplikacjach przez niego eksploatowanych w organizacji,

1. dokumentami – w tym zakresie oprogramowanie musi:

* posiadać rejestr wszystkich dokumentów określających wymagania (m.in.: polityk, zarządzeń, decyzji, instrukcji, procedur) obowiązujących na poszczególnych stanowiskach pracy w urzędzie,
* posiadać możliwość opisania dokumentu poprzez m.in.: określenie osoby odpowiedzialnej za dokument, przypisanie do procesu, który realizuje oraz wskazanie właściwych stanowisk pracy na jakich obowiązuje,
* posiadać możliwość udostępniania treści dokumentu pracownikom,
* posiadać możliwość elektronicznego wnioskowania o utworzenie bądź zmianę dokumentu, nadzorowania etapów jego tworzenia oraz opiniowania przez wytypowanych użytkowników przesłanego projektu dokumentu,
* posiadać możliwość dystrybucji zatwierdzonego dokumentu na stanowiska pracy, na których obowiązuje dokument,
* posiadać możliwość elektronicznego zapoznania się przez użytkownika, będącego jednocześnie pracownikiem urzędu, z dokumentem obowiązującym na zajmowanym przez niego stanowisku pracy i elektronicznego potwierdzenia zapoznania się z treścią dokumentu,
* posiadać narzędzia weryfikacji danych dotyczących potwierdzenia zapoznania pracowników z dokumentacją obowiązującą na ich stanowisku pracy,

1. założeniami wdrożonego w Urzędzie SZBI – w tym zakresie oprogramowanie musi:

* wspomagać opisywanie kontekstu organizacji w tym dokumentować okresowe analizy czynników mających wpływ na zdolność organizacji do osiągania zamierzonych celów, umożliwiać opisanie zakresu i wyłączeń systemu oraz potrzeb i oczekiwań stron zainteresowanych,
* udostępniać pracownikom przygotowaną w programie deklarację polityki bezpieczeństwa informacji wraz ze spójnymi z nią celami powiązanymi
* z procesami oraz wskaźnikami ich pomiarów,
* w sposób przejrzysty udostępniać pracownikom organizacji pełne wymagania systemu zarządzania bezpieczeństwem informacji i ochrony danych osobowych, w tym prezentować w formie graficznej wzajemne powiązania dokumentacji (tworzyć interaktywny schemat z możliwością otwierania poszczególnych dokumentów po kliknięciu na elementy grafu).

1. sprzętem komputerowym i oprogramowaniem komputerowym – w tym zakresie oprogramowanie musi:

* posiadać rejestr wszystkich urządzeń informatycznych oraz zainstalowanego na nim oprogramowania komputerowego,
* mieć możliwość automatycznego sczytywania parametrów sprzętowych
* i oprogramowania zainstalowanego na komputerach działających pod kontrolą systemu operacyjnego Windows,
* posiadać możliwość ewidencjonowania bieżących przeglądów sprzętu komputerowego oraz zainstalowanego na nim oprogramowania,
* posiadać możliwość elektronicznego zgłaszania usterek i awarii sprzętu komputerowego,
* posiadać możliwość ewidencjonowania rodzaju umów serwisowych na sprzęt komputerowy,
* posiadać możliwość ewidencjonowania i zarządzania materiałami eksploatacyjnymi niezbędnymi do pracy sprzętów komputerowych np. tonery do drukarek,
* posiadać możliwość ewidencji wszystkich zdarzeń, czynności naprawczych, serwisowych czy konserwacyjnych komputerów lub serwera.

1. licencjami na oprogramowanie – w tym zakresie oprogramowanie musi:

* posiadać rejestr licencji oprogramowania komputerowego zainstalowanego na komputerach w Urzędzie oraz rejestr umów licencyjnych podpisanych przez Urząd na dostawę specjalistycznego oprogramowania,
* posiadać możliwość ewidencji posiadanych przez Urząd umów na korzystanie z licencji programów komputerowych,

1. obsługą problemów zgłaszanych przez użytkowników – w tym zakresie oprogramowanie musi:

* dostarczać użytkownikom kanał komunikacji do zgłaszania problemów z obszaru IT,
* dokumentować obsługę zgłoszeń oraz nadzorować terminowości ich realizacji,
* określać kategorie zgłoszeń i ustalać osoby odpowiedzialne za ich obsługę,

1. aktywami informacyjnymi – w tym zakresie oprogramowanie musi:

* umożliwiać prowadzenie rejestru zidentyfikowanych aktywów informacyjnych oraz zasobów wspomagających,
* wspomagać opisywanie aktywów m.in. poprzez wskazanie procesów przetwarzających informacje oraz istotności informacji dla realizacji danego procesu, wskazanie zasobów wykorzystywanych przy przetwarzaniu informacji oraz określenie poziomu istotności zasobu dla informacji,
* umożliwiać ustalenie wymaganego poziomu podstawowych oraz dodatkowych atrybutów informacji i adekwatnie do tego ustalać klasyfikacje aktywów.

1. zarządzania uprawnieniami użytkowników w aplikacjach – w tym zakresie oprogramowanie musi:

* posiadać rejestr wszystkich aplikacji użytkowanych w Urzędzie,
* posiadać rejestr nadanych w Urzędzie uprawnień do przetwarzania danych w aplikacjach komputerowych zgodnie z zakresem zadań wykonywanych przez pracownika,
* posiadać możliwość elektronicznego wnioskowania o nadanie właściwych uprawnień dla pracowników zgodnie z ich zakresem obowiązków do obsługi programów komputerowych, w których są przetwarzane dane osobowe,
* w przypadku aplikacji przetwarzających dane osobowe weryfikować, czy pracownik posiada upoważnienie do przetwarzania danych osobowych,
* ustalać etapy przetwarzania wniosku m.in. akceptację, opiniowanie zatwierdzanie,
* informować użytkowników odpowiedzialnych za realizację danego etapu przetwarzania wniosku o konieczności jego zrealizowania,
* posiadać możliwość elektronicznego potwierdzenia przez pracownika zapoznania się z zakresem nadanego uprawnienia,

1. incydentami i słabościami systemu – w tym zakresie oprogramowanie musi:

* posiadać rejestr zaistniałych incydentów oraz słabości systemu,
* podsiadać możliwość zgłoszenia zidentyfikowanego zdarzenia lub słabości systemu bezpieczeństwa informacji (w tym naruszenia ochrony danych osobowych),
* umożliwiać analizę i klasyfikację zgłoszonego zdarzenia,
* wspomagać obsługę incydentów bezpieczeństwa informacji w tym określenia operatora incydentu oraz ewidencjonować podejmowane działania,
* posiadać stosowne zestawienia dotyczące zidentyfikowanych incydentów i słabości systemów w Urzędzie,

1. certyfikatami bezpieczeństwa – w tym zakresie oprogramowanie musi:

* posiadać rejestr certyfikatów bezpieczeństwa,
* posiadać możliwość wnioskowania o nadanie certyfikatu bezpieczeństwa,
* umożliwiać użytkownikom uprawnionym ewidencjonowanie certyfikatów bezpieczeństwa,
* umożliwiać elektroniczne potwierdzenia posiadania przez pracownika certyfikatu bezpieczeństwa,
* informować użytkowników uprawnionych o zbliżającym się terminie ważności certyfikatu i nadzorować etapy jego odnowienia,
* posiadać możliwość unieważniania certyfikatu bezpieczeństwa,

1. wewnętrznymi audytami w zakresie bezpieczeństwa informacji i ochroną danych osobowych – w tym zakresie oprogramowanie musi:

* posiadać rejestr przeprowadzonych w Urzędzie audytów wewnętrznych w tym audytów w zakresie bezpieczeństwa informacji i ochrony danych osobowych,
* posiadać możliwość tworzenia programów audytów wewnętrznych na danych rok oraz planowania audytów z określeniem m.in.: zakresu audytu, przedmiotu audytu, komórek organizacyjnych uczestniczących w działaniach audytowych, terminu przeprowadzenia audytu oraz osób przeprowadzających audyt,
* możliwość dokumentowania podjętych działań audytowych tj. przygotowanie m.in.: programu audytów na dany rok, protokołu końcowego z audytu,
* możliwość dokumentowania wszystkich spostrzeżeń, niezgodności i wniosków wynikłych podczas podjętych działań audytowych,
* możliwość zgłoszenia zauważonych podczas audytu niezgodności do właściwej osoby odpowiedzialnej,

1. działaniami doskonalącymi – w tym zakresie oprogramowanie musi:

* posiadać rejestr wszystkich zidentyfikowanych w Urzędzie nieprawidłowości (niezgodności) w zakresie bezpieczeństwa informacji i ochrony danych osobowych,
* posiadać możliwość elektronicznego zgłaszania zidentyfikowanych nieprawidłowości w funkcjonowaniu systemu bezpieczeństwa informacji
* i ochrony danych osobowych,
* możliwość analizy zgłoszonej nieprawidłowości przez osoby za to odpowiedzialne,
* możliwość określenia działań korygujących i korekcyjnych względem zidentyfikowanej nieprawidłowości oraz głoszenia wykonania działań korygujących,

1. przeglądami zarządzania w zakresie bezpieczeństwa informacji i ochroną danych osobowych – w tym zakresie oprogramowanie musi:

* posiadać rejestr przeprowadzanych w Urzędzie cyklicznych przeglądów zarządzania w zakresie m.in. bezpieczeństwa informacji i ochrony danych osobowych,
* możliwość automatycznego przygotowania raportu do analizy z zakresu m.in. bezpieczeństwa informacji i ochrony danych osobowych.

1. Wszystkie moduły programu muszą być ze sobą kompatybilne i wzajemnie powiązane (moduły powinny korzystać z danych wprowadzanych w innych modułach bez konieczności ponownego ewidencjonowania tych samych danych).
2. Program musi informować użytkownika o działaniach, które musi podjąć w aplikacji ze względu na posiadane w aplikacji uprawnienia lub zajmowane w organizacji stanowisko pracy.
3. Komunikaty adresowane do użytkowników muszą być dostępne po zalogowaniu użytkownika do bezpośrednio aplikacji i w formie powiadomień PUSH oraz równolegle wysyłane na adres e-mail użytkownika.
4. Z poziomu komunikatu przesłanego pocztą elektroniczną użytkownik może przejść bezpośrednio do modułu w programie, w którym musi podjąć działania.
5. **Licencja**
6. Licencja ma być przyznana na czas nieograniczony.
7. Licencja ma zezwalać na jednoczesną pracę w programie wszystkich pracowników Urzędu.
8. Licencja nie może ograniczać liczby końcówek jednocześnie korzystających z oprogramowania.
9. Licencja musi dopuszczać tworzenie przez Zamawiającego dowolnej ilości kopii oprogramowania dla celów testowych lub szkoleniowych.
10. Aktualizacja SZBI - usługa
11. **Zakres zamówienia i etapy realizacji**
12. **Analiza stanu obecnego (audyt wstępny):** Wykonawca przeprowadzi przegląd bieżących praktyk w obszarze bezpieczeństwa informacji w Gminie Wodzisław obejmie to analizę istniejącej dokumentacji z zakresu bezpieczeństwa informacji i ochrony danych osobowych, ocenę stosowanych zabezpieczeń technicznych i organizacyjnych, a także identyfikację ewentualnych luk czy niezgodności względem norm i przepisów.
13. **Opracowanie/aktualizacja dokumentacji SZBI:** Na podstawie wyników analizy Wykonawca dokona aktualizacji istniejącej dokumentacji bezpieczeństwa informacji. W przypadku braku wymaganych dokumentów – zostaną one opracowane od podstaw. Dokumentacja ma być zgodna z wymaganiami norm rodziny ISO 27000 lub równoważnych (w szczególności z normą PN-EN ISO/IEC 27001:2023 dotyczącą systemów zarządzania bezpieczeństwem informacji, z uwzględnieniem zaleceń norm PN-ISO/IEC 27002 oraz PN-ISO/IEC 27005) oraz z normą ISO 31000 (zarządzanie ryzykiem) i – w zakresie ciągłości działania – z normą ISO 22301 (zarządzanie ciągłością działania). Celem jest zapewnienie, że SZBI będzie spełniał wymagania Krajowych Ram Interoperacyjności (KRI), ustawy o KSC oraz RODO. Dokumentacja musi zawierać wszystkie niezbędne polityki i procedury dostosowane do specyfiki Zamawiającego, w tym m.in.: Politykę Bezpieczeństwa Informacji, instrukcje, wytyczne, rejestry, wzory dokumentów oraz metodykę zarządzania ryzykiem. Wykonawca ma dostarczyć spójną, kompletną i czytelną dokumentację SZBI, obejmującą cały zakres wymagany powołanymi normami i przepisami.
14. **Szczegółowe polityki, procedury i instrukcje:** w ramach dokumentacji z pkt 2 wykonawca zaktualizuje, a w przypadku braku opracuje wymagane polityki tematyczne, procedury, instrukcje oraz elementy dokumentacji operacyjnej, adekwatnie do potrzeb organizacji, pokrywające wszystkie kluczowe obszary bezpieczeństwa informacji. Poniżej przedstawiono minimalny zakres obszarów, które dokumentacja SZBI powinna objąć (w nawiasach podano przykładowe elementy każdej polityki/procedury):
    1. Zarządzanie tożsamością i dostępem – zasady przydzielania i odbierania uprawnień dostępu do systemów i danych, procedury rejestracji, zmian i likwidacji dostępów użytkowników, mechanizmy autoryzacji użytkowników w systemach informatycznych.
    2. Bezpieczeństwo personelu (zarządzanie zasobami ludzkimi) – procedury bezpieczeństwa przy rekrutacji, w okresie zatrudnienia i zakańczania współpracy, obowiązki w zakresie bezpieczeństwa informacji nałożone na personel, szkolenia wstępne z zasad bezpieczeństwa.
    3. Świadomość i szkolenia – program podnoszenia świadomości bezpieczeństwa informacji wśród pracowników, plan szkoleń z zakresu cyberbezpieczeństwa oraz monitorowanie wiedzy personelu na temat zagrożeń i dobrych praktyk.
    4. Zarządzanie aktywami informacyjnymi – rejestr zasobów informacyjnych (aktywa informacyjne), klasyfikacja informacji, zasady użytkowania i ochrony sprzętu oraz nośników danych.
    5. Bezpieczeństwo fizyczne i środowiskowe – zabezpieczenia fizyczne budynków i pomieszczeń (kontrola dostępu, monitoring, ochrona przeciwpożarowa itp.), zapewnienie bezpiecznych warunków środowiskowych dla aktywów i infrastruktury teleinformatycznej.
    6. Bezpieczeństwo systemów informatycznych i sieci – wytyczne bezpiecznej konfiguracji systemów i urządzeń sieciowych, zarządzanie zmianami w systemach, zabezpieczenia sieci (firewalle, systemy wykrywania włamań), polityka aktualizacji oprogramowania (łat bezpieczeństwa).
    7. Bezpieczna konfiguracja i bezpieczeństwo aplikacji – standardy konfiguracyjne dla elementów infrastruktury IT, zasady tworzenia i utrzymania bezpiecznej konfiguracji (hardening), wymagania bezpieczeństwa przy tworzeniu lub nabywaniu oprogramowania, testowanie aplikacji pod kątem podatności.
    8. Ochrona informacji i kryptografia – procedury ochrony informacji poufnych, w tym danych osobowych szczególnej kategorii , zasady szyfrowania danych i komunikacji, polityka haseł i zarządzanie kluczami kryptograficznymi, bezpieczne tworzenie kopii zapasowych (backup) i odtwarzanie danych.
    9. Zarządzanie incydentami bezpieczeństwa informacji – procedura zgłaszania incydentów przez pracowników, rejestrowania i monitorowania incydentów; proces reagowania na incydenty (rola zespołu reagowania, działania doraźne, eskalacja); post-incident review – analiza przyczyn incydentu i wyciąganie wniosków.
    10. Zarządzanie ciągłością działania – polityka ciągłości i procedura utrzymania ciągłości działania (BCP) na wypadek poważnych awarii lub incydentów, procedury awaryjne, planowanie odtwarzania kluczowych usług; testowanie planów ciągłości i dokonywanie ich przeglądów.
    11. Zarządzanie ryzykiem – metodyka identyfikacji ryzyk dla bezpieczeństwa informacji, analiza ryzyka (oszacowanie prawdopodobieństwa i wpływu potencjalnych zagrożeń), określenie akceptowalnego poziomu ryzyka; plany postępowania z ryzykiem (wybór sposobu traktowania ryzyka: akceptacja, redukcja, unikanie, przeniesienie) oraz regularne przeglądy i aktualizacja analizy ryzyka.
    12. Bezpieczeństwo relacji z dostawcami – polityka zarządzania bezpieczeństwem łańcucha dostaw IT; zasady włączania wymagań bezpieczeństwa do umów z dostawcami; procedura weryfikacji i nadzoru dostawców pod kątem spełniania standardów bezpieczeństwa informacji przez podmioty zewnętrzne.
    13. Monitorowanie, przeglądy i audyty wewnętrzne SZBI – ustanowienie procesu ciągłego monitorowania systemów i sieci pod kątem incydentów i naruszeń; harmonogram i zakres regularnych audytów wewnętrznych SZBI (np. rocznych) oraz przeglądów zarządzania SZBI przez kierownictwo; zarządzanie niezgodnościami i działaniami korygującymi (procedura dokumentowania stwierdzonych niezgodności, wyznaczania działań korygujących/zapobiegawczych oraz monitorowania ich wdrożenia).
    14. Zarządzanie dokumentacją bezpieczeństwa – zasady tworzenia, zatwierdzania, wersjonowania i dystrybucji dokumentów SZBI; utrzymanie rejestru dokumentacji; kontrola dostępu do dokumentacji, znakowanie dokumentów (klauzule tajności, klauzule publiczne); polityka archiwizacji i okresowego przeglądu dokumentacji pod kątem aktualności. Uwaga: Powyższa lista ma charakter minimum – Wykonawca jest zobowiązany dostosować i rozwinąć dokumentację według faktycznych potrzeb Zamawiającego, tak aby żaden istotny obszar bezpieczeństwa informacji nie został pominięty. Wszystkie dokumenty powinny być ze sobą spójne, tworzyć zintegrowany System Bezpieczeństwa Informacji.
15. **Wdrożenie dokumentacji i praktyk SZBI:** Po opracowaniu kompletu dokumentów Wykonawca będzie wspomagał w organizacji proces wdrożenia SZBI. Obejmuje to, komunikację nowych zasad wybranym pracownikom oraz instruktaż dla personelu odpowiedzialnego za poszczególne obszary (np. Pełnomocnika ds. Systemu Zarządzania Bezpieczeństwem Informacji / Inspektora Ochrony Danych, Administratorów Systemów IT, kadry kierowniczej). Wykonawca zapewni wsparcie we wprowadzaniu nowych rozwiązań organizacyjno-technicznych, tak by SZBI faktycznie zaczął funkcjonować w praktyce.
16. **Warunki jakościowe dotyczące dokumentacji:** Zamawiający nie dopuszcza kopiowania ogólnodostępnych wzorców dokumentów bezpieczeństwa w formie nieprzetworzonej. Wszelkie treści zapożyczone (np. fragmenty norm, przepisów, publikacji) powinny być przywoływane (referencje) zamiast dosłownego cytowania. Dokumentacja musi stanowić oryginalne opracowanie wykonane przez Wykonawcę w ramach realizacji zamówienia – dostosowane do specyfiki organizacji i wyczerpujące w kontekście celu, jakiemu ma służyć. Niedopuszczalne jest dostarczenie uniwersalnych „szablonów" bez odpowiedniej personalizacji; Zamawiający wymaga, aby wszystkie polityki, procedury i instrukcje uwzględniały konkretne uwarunkowania Gminy Wodzisław (strukturę organizacyjną, zakres działań, posiadane systemy informatyczne, ryzyka charakterystyczne dla danej jednostki itp.).
17. **Wymagania organizacyjne i prawne**
18. **Zgodność z przepisami i normami:** Wykonawca jest zobowiązany zrealizować przedmiot zamówienia z uwzględnieniem wszelkich obowiązujących przepisów prawa i norm związanych z bezpieczeństwem informacji. W szczególności rezultat projektu musi spełniać wymagania:
    1. Ustawy o krajowym systemie cyberbezpieczeństwa (KSC) – w zakresie nałożonych na podmiot publiczny obowiązków dotyczących cyberbezpieczeństwa (m.in. posiadanie procedur zgłaszania incydentów, wyznaczenie osoby kontaktowej ds. cyberbezpieczeństwa, przeprowadzanie audytu co 2 lata itp.).
    2. Rozporządzenia w sprawie Krajowych Ram Interoperacyjności (KRI) – w zakresie minimalnych wymagań dla systemów teleinformatycznych w administracji publicznej, polityki bezpieczeństwa informacji, planów ciągłości działania, ochrony przed szkodliwym oprogramowaniem, bieżącego monitorowania bezpieczeństwa oraz przeprowadzania okresowych audytów.
    3. Rozporządzenia UE 2016/679 (RODO) – w zakresie ochrony danych osobowych. Dokumentacja SZBI oraz wdrożone procedury muszą zapewniać zgodność z RODO, m.in. poprzez uwzględnienie zasad privacy by design, prowadzenie rejestru czynności przetwarzania (jeśli dotyczy), zabezpieczenie danych osobowych na poziomie odpowiadającym ryzyku.
    4. Norm PN-EN ISO/IEC 27001:2023 oraz pokrewnych – efekt wdrożenia powinien odpowiadać wymaganiom ISO 27001 (punktom normy dotyczącym ustanowienia polityk, ról, analizy ryzyka, kontroli z Załącznika A itd.), a także uwzględniać wytyczne ISO/IEC 27002 (dobre praktyki zabezpieczeń) i ISO/IEC 27005 (zarządzanie ryzykiem). Deklaracja zgodności z kontrolami ISO 27001 powinna zostać opracowana i zawierać uzasadnienie wdrożenia bądź wykluczenia poszczególnych zabezpieczeń.
    5. Norma ISO 22301 (ciągłość działania) – w zakresie zapewnienia ciągłości działania dla infrastruktury teleinformatycznej kluczowej dla przetwarzania informacji (np. serwerów). Wymaga się, aby w ramach SZBI uwzględniono elementy systemu zarządzania ciągłością działania lub powiązano SZBI z funkcjonującym Planem Ciągłości Działania Starostwa.

Wszystkie prace muszą być wykonane zgodnie z zasadami sztuki, rzetelnie i z dochowaniem należytej staranności profesjonalnej.

1. **Niezależność i poufność:** Wykonawca zobowiązuje się do zachowania poufności wszelkich informacji uzyskanych w trakcie realizacji zamówienia. Przed rozpoczęciem prac przystąpi do stosownych umów o zachowaniu poufności (NDA) z Zamawiającym. Audytorzy i konsultanci Wykonawcy muszą być niezależni od audytowanych obszarów – nie mogą być pracownikami ani związani w sposób mogący rodzić konflikt interesów z żadną z jednostek objętych projektem. Wykonawca gwarantuje, że wyniki audytu będą obiektywne.
2. **Współpraca z Zamawiającym:** Zamawiający zapewni dostęp do niezbędnych informacji, dokumentów i personelu na potrzeby realizacji zamówienia. Wykonawca w uzgodnieniu z Zamawiającym opracuje szczegółowy harmonogram prac, uwzględniający etapy: analizy, opracowywania dokumentów, wdrożenia oraz audytu. W ramach realizacji wymaga się odbywania regularnych spotkań statusowych (np. raz na dwa tygodnie) celem omówienia postępów prac. Wykonawca przekaże Zamawiającemu wszelkie opracowane dokumenty również w formie edytowalnej (format Microsoft Word/Excel).
3. **Ochrona praw autorskich:** Wszystkie utwory stworzone w wyniku realizacji zamówienia (dokumentacja SZBI, raporty, materiały szkoleniowe itp.) będą objęte majątkowymi prawami autorskimi przeniesionymi na Zamawiającego na zasadach określonych w umowie. Wykonawca zapewnia, że dostarczone materiały nie naruszają praw osób trzecich i że posiada uprawnienia do dysponowania nimi.
4. **Harmonogram prac:** W ciągu 10 dni od podpisania umowy Wykonawca przedstawi do akceptacji Zamawiającego harmonogram prac uwzględniający wszystkie założenia projektu.
5. **Wymagania wobec Wykonawcy (kwalifikacje i doświadczenie)**

Zamawiający stawia następujące minimalne warunki udziału w postępowaniu dotyczące doświadczenia wykonawcy oraz składu i kwalifikacji kluczowego personelu, który będzie realizował zamówienie:

1. **Doświadczenie Wykonawcy w zakresie SZBI:** Wykonawca musi wykazać, że w okresie ostatnich 3 lat (licząc wstecz od dnia upływu terminu składania ofert), jeżeli okres prowadzenia jest krótszy to w czasie, zrealizował należycie co najmniej 5 usług polegających na opracowaniu i wdrożeniu Systemu Zarządzania Bezpieczeństwem Informacji. Każda z tych usług powinna mieć wartość co najmniej 30 000 zł brutto. Warunek ilościowy podyktowany jest potrzebą zapewnienia, iż Wykonawca posiada praktyczne doświadczenie w kompleksowym wdrażaniu SZBI.
2. **Doświadczenie Wykonawcy w zakresie audytów KSC/ISO 27001:** Wykonawca musi wykazać, że w okresie ostatnich 3 lat, jeżeli okres prowadzenia działalności jest krótszy to w tym czasie, zrealizował co najmniej 5 usług polegających na przeprowadzeniu audytu bezpieczeństwa informacji (audytu zgodności z KRI lub normą ISO 27001) oraz sporządzeniu Ankiety Dojrzałości Cyberbezpieczeństwa JST. Każdy audyt musi mieć wartość co najmniej 8 000 zł brutto. Usługi audytorskie muszą być wykonane na rzecz podmiotów sektora finansów publicznych (preferencyjnie w jednostkach samorządu terytorialnego) i potwierdzać znajomość specyfiki audytów wymaganych w projektach dofinansowanych z programu „Cyberbezpieczny Samorząd".
3. **Kwalifikacje zespołu projektowego:** Wykonawca musi dysponować zespołem specjalistów zdolnych do realizacji zamówienia, w tym co najmniej następującymi osobami (które będą bezpośrednio zaangażowane w wykonanie zamówienia):
   1. Kierownik Zespołu Projektowego (1 osoba): Wymagane wykształcenie wyższe. Certyfikat PRINCE2 Practitioner lub równoważny, potwierdzający znajomość metodyk zarządzania projektami. Dodatkowo Kierownik projektu powinien posiadać co najmniej certyfikat Audytora wewnętrznego SZBI wg PN-EN ISO/IEC 27001:2023 (wydany przez akredytowaną jednostkę certyfikującą osoby) – co potwierdza znajomość standardów bezpieczeństwa informacji. Osoba ta powinna mieć doświadczenie w pełnieniu roli kierownika projektu przy realizacji co najmniej dwóch projektów finansowanych ze źródeł zewnętrznych (UE lub budżet państwa). Będzie odpowiedzialna za nadzór nad całością prac, kontakt z Zamawiającym oraz zarządzanie ryzykiem projektowym.
   2. Audytor Wiodący ds. Bezpieczeństwa Informacji (min. 3 osoby): Wymagane wykształcenie wyższe oraz wiedza z zakresu funkcjonowania procesów bezpieczeństwa w administracji publicznej. Każda z tych osób musi posiadać uprawnienia określone w § 2 ust. 1 Rozporządzenia Ministra Cyfryzacji z 12 października 2018 r. (Dz.U. 2018 poz. 1999) – czyli co najmniej jeden z certyfikatów uprawniających do przeprowadzania audytów KSC (np. Certified Lead Auditor ISO 27001, CISA, CISM, CRISC, CISSP – o ile dany certyfikat znajduje się w wykazie rozporządzenia). Wymagane jest doświadczenie: udział (jako audytor wiodący lub członek zespołu) w min. 3 projektach zrealizowanych w ostatnich 3 latach, obejmujących wdrożenie SZBI oraz wykonanie audytu bezpieczeństwa informacji w jednostkach samorządu terytorialnego. Co najmniej jedna z osób na stanowisku Audytora Wiodącego musi dodatkowo posiadać certyfikat z zakresu ochrony danych osobowych (np. Inspektor Ochrony Danych, CIPP/E lub równoważny), aby zapewnić specjalistyczną wiedzę odnośnie RODO w zespole.
   3. Audytor Wewnętrzny ds. Bezpieczeństwa Informacji (min. 2 osoby): Wymagane wykształcenie wyższe oraz praktyczna znajomość procesów bezpieczeństwa w sektorze publicznym. Każda z tych osób powinna legitymować się certyfikatem Audytora wewnętrznego SZBI wg normy ISO/IEC 27001 (wydanym przez akredytowaną jednostkę certyfikującą). Doświadczenie: udział w co najmniej 2 zakończonych projektach (w ciągu ostatnich 3 lat) obejmujących wdrożenie SZBI i/lub przeprowadzenie audytu bezpieczeństwa informacji w JST. Audytorzy wewnętrzni będą odpowiedzialni za bieżące prace analityczne, przygotowanie dokumentacji, wykonywanie audytów cząstkowych oraz wsparcie Audytorów Wiodących.
   4. Specjalista ds. Technicznych (Cyberbezpieczeństwo IT) – 1 osoba: Wymagane wykształcenie wyższe (preferowane informatyczne). Certyfikat CISSP (Certified Information Systems Security Professional) lub równoważny, potwierdzający rozległą wiedzę techniczną z zakresu bezpieczeństwa systemów i sieci. Osoba ta powinna mieć doświadczenie w przeprowadzaniu audytów bezpieczeństwa systemów informatycznych – wymagany udział w co najmniej 2 audytach technicznych (testy bezpieczeństwa, przegląd konfiguracji systemów itp.) w JST w ostatnich 3 latach. Specjalista ten wesprze zespół od strony technicznej, m.in. przy analizie konfiguracji sprzętu i oprogramowania, ocenie podatności, rekomendowaniu rozwiązań technicznych (firewalle, systemy backup, systemy SIEM etc.).
   5. Audytor Wiodący Systemu Zarządzania Ciągłością Działania (BCMS) – 1 osoba: Wymagane wykształcenie wyższe. Certyfikat Audytora Wiodącego BCMS wg ISO 22301:2020 (wydany przez akredytowaną jednostkę certyfikującą osoby) potwierdzający kompetencje w obszarze ciągłości działania. Wymagana wiedza z zakresu analizy wpływu na ciągłość działania (Business Impact Analysis), planowania i testowania strategii ciągłości działania w sektorze publicznym. Doświadczenie: udział w co najmniej 1 projekcie w ciągu ostatnich 3 lat obejmującym audyt lub wdrożenie systemu ciągłości działania w JST lub instytucji publicznej. Rola tej osoby to zapewnienie, że aspekt ciągłości działania (wymagany przepisami KRI i dobrą praktyką ISO 27001) zostanie prawidłowo uwzględniony przy wdrażaniu SZBI i w audycie końcowym.

Uwaga: Jedna osoba może łączyć role, o ile posiada wymagane kwalifikacje dla każdej z nich (np. Audytor Wiodący może jednocześnie być Audytorem BCMS, jeśli ma oba certyfikaty). Jednak minimalny skład zespołu musi obejmować przynajmniej 5 różnych osob wskazanych powyżej, aby zapewnić odpowiednią obsadę (przy czym Audytorów Wiodących ds. Bezpieczeństwa wymaganych jest trzech niezależnych ekspertów).

1. **Ubezpieczenie OC wykonawcy:** Wykonawca musi posiadać aktualne ubezpieczenie odpowiedzialności cywilnej w zakresie prowadzonej działalności gospodarczej, obejmujące szkody mogące powstać w związku z realizacją niniejszego zamówienia. Suma gwarancyjna polisy powinna wynosić co najmniej 150 000,00 zł na jedno i wszystkie zdarzenia. Potwierdzenie posiadania takiego ubezpieczenia (kopia polisy wraz z dowodem opłacenia składki) należy dołączyć do oferty. W przypadku wyboru oferty, Wykonawca zobowiązuje się utrzymywać ciągłość ubezpieczenia przez cały okres trwania umowy oraz – na żądanie – przedstawiać do wglądu aktualne dokumenty potwierdzające ubezpieczenie.
2. Audyt końcowy SZBI
3. **Audyt zgodności SZBI:** Po zakończeniu etapu wdrożenia SZBI i po okresie jego stabilnego funkcjonowania, zostanie przeprowadzony końcowy audyt SZBI. Audyt ma na celu niezależną ocenę zgodności wdrożonego systemu zarządzania bezpieczeństwem informacji z przyjętymi wymaganiami. Zakres audytu będzie obejmował w szczególności sprawdzenie zgodności z:
   1. Kryteriami zawartymi w § 19 ust. 2 Rozporządzenia Rady Ministrów z dnia 21 maja 2024 r. w sprawie Krajowych Ram Interoperacyjności (Dz.U. 2024 poz. 773) lub
   2. Równoważnie: wymaganiami normy PN-ISO/IEC 27001:2023 (system zarządzania bezpieczeństwem informacji).

Uwaga: Powyższe dwie podstawy są zbieżne (norma ISO 27001 pokrywa w dużej mierze wymagania KRI), dlatego audyt będzie zaprojektowany tak, by ocenić zgodność SZBI zarówno z krajowymi przepisami (KRI, ustawa o KSC) jak i z międzynarodową normą przy jednoczesnym zebraniu informacji pozwalających na opracowanie Ankiety dojrzałości cyberbezpieczeństwa JST.

1. **Zakres podmiotowy audytu:** Audyt końcowy obejmie Gminę Wodzisław.
2. **Wymogi dotyczące audytorów:** Audyt musi zostać przeprowadzony przez audytorów posiadających uprawnienia zgodne z przepisami. Wymagane jest, by w skład zespołu audytującego wchodziła co najmniej jedna osoba posiadająca certyfikat uprawniający do przeprowadzania audytów w myśl Rozporządzenia Ministra Cyfryzacji z dnia 12 października 2018 r. (Dz.U. 2018 poz. 1999). Oznacza to, że audytor wiodący musi legitymować się np. certyfikatem Lead Auditor ISO/IEC 27001, CISA, CISM lub innym wymienionym w załączniku do ww. rozporządzenia. Wszyscy audytorzy powinni mieć doświadczenie w audytach systemów bezpieczeństwa informacji, a przynajmniej jeden audytor powinien znać specyfikę sektora publicznego (administracji samorządowej).
3. **Metodyka audytu:** Audyt zostanie przeprowadzony według uznanych standardów audytorskich – obejmie przegląd dokumentacji SZBI, wywiady z kluczowym personelem (w tym Kierownictwem Urzędu, osobami odpowiedzialnymi za poszczególne obszary bezpieczeństwa informacji takimi jak Administratorzy Systemów Informatycznych, Pełnomocnik ds. SZBI, , kierownikami jednostek organizacyjnych), oraz testy zgodności w praktyce (sprawdzenie próbek zapisów, rejestrów incydentów, ustawień systemów itp.). Audytorzy przygotują Raporty z audytu (osobne raporty dla każdej z audytowanych jednostek), które będą zawierały:
4. Opis stanu zastanego (opis funkcjonujących mechanizmów kontroli i zabezpieczeń).
5. Wskazanie stwierdzonych niezgodności lub obszarów wymagających ulepszeń, wraz z rekomendacjami działań naprawczych.
6. Ocenę poziomu zgodności z wymaganiami.

Raport musi być przekazany Zamawiającemu elektronicznej podpisany przez Audytora posiadającego odpowiednie uprawnienia.

1. **Ankieta dojrzałości cyberbezpieczeństwa JST:** Integralnym rezultatem audytu będzie wypełnienie standaryzowanej Ankiety Dojrzałości Cyberbezpieczeństwa. Jest to dokument (ankieta) określony w dokumentacji konkursu grantowego „Cyberbezpieczny Samorząd" – stanowi załącznik nr 6 do Regulaminu konkursu. Wykonawca (audytor) wypełni tę ankietę zgodnie z ustaleniami audytu, obiektywnie oceniając poziom dojrzałości Gminy Wodzisław w obszarze cyberbezpieczeństwa po zrealizowaniu projektu. Wykonawca przekaże Zamawiającemu wypełniony plik ankiety, co będzie stanowiło potwierdzenie wykonania zadania wymaganego przez Instytucję Zarządzającą projektem.
2. **Udział w procesie oceny i rozliczenia projektu:** W razie potrzeby Wykonawca udzieli Zamawiającemu dodatkowych wyjaśnień dotyczących wyników audytu i rekomendacji. Może to obejmować np. uczestnictwo w spotkaniu podsumowującym z kierownictwem Gminy Wodzisław, konsultacje przy tworzeniu ewentualnych działań naprawczych poaudytowych, a także wsparcie przy przygotowaniu dokumentów związanych z rozliczeniem grantu (jeśli instytucja grantodawcza będzie miała pytania co do audytu lub ankiety).
3. **Termin realizacji:** Audyt końcowy zostanie przeprowadzony w terminie nie dłużej niż do końca 2025 roku. Dokładny termin audytu zależeć będzie od gotowości organizacji do poddania się ocenie – przyjmuje się, że audyt odbędzie się przed złożeniem przez Zamawiającego wniosku o płatność końcową w projekcie. Zamawiający powiadomi Wykonawcę pisemnie (drogą e-mail) o gotowości do audytu z odpowiednim wyprzedzeniem, uzgadniając szczegółowy harmonogram prac audytowych.
4. Zakup dostępu do platformy szkoleniowej z zakresu cyberbezpieczeństwa dla pracowników urzędu kpl.1

Przedmiotem zamówienia jest zakup dostępu do platformy szkoleniowej, na której pracownicy będą mogli na bieżąco szkolić się z zakresu cyberbezpieczeństwa.

W ramach realizacji zamówienia Wykonawca zobowiązany będzie do zapewnienia pracownikom Zamawiającego **dostępu do** **platformy szkoleniowej** dla pracowników na okres 6 miesięcy. Na platformie szkoleniowej (e-learningowej) zamieszczone będą różnorodne materiały szkoleniowe z zakresu cyberbezpieczeństwa. Materiały szkoleniowe muszą być przez Wykonawcę na bieżąco uzupełniane i aktualizowane, w związku z pojawianiem się nowych zagrożeń i podatności, nowych metod ochrony informacji i narzędzie do tego wykorzystywanych oraz zmieniającej się sytuacji geopolitycznej.

Udostępnienie platformy e-learningowej ma umożliwić pracownikom elastyczny dostęp do aktualnych informacji i standardowych praktyk w dogodnym dla nich czasie, co będzie sprzyjać skutecznej nauce, oraz poszerzenia wiedzy o inne tematy związane z cyberbezpieczeństwem.

Liczba użytkowników platformy – min. 40.

Platforma musi spełniać następujące wymagania:

1. Zawierać minimum 45 szkoleń, dostępnych w języku polskim, w postaci filmów i prezentacji, zakończonych testami lub quizami sprawdzającymi przyswojenie przedstawianego materiału merytorycznego.
   1. Szkolenia muszą zapewniać zakres tematyczny co najmniej w ujęciu:
   * Podstawy bezpiecznego internetu
   * Bezpieczeństwo poczty
   * Załączniki w poczcie elektronicznej
   * Phishing
   * Spyware/malware
   * Bezpieczeństwo danych osobowych RODO/GDRP
   * Bezpieczne hasła
   * Menedżery haseł
   * Bezpieczeństwo urządzeń mobilnych
   * Uwierzytelnianie wieloskładnikowe (MFA)
   * Bezpieczna praca zdalna
   * Bezpieczna praca w biurze
   * Sieci społeczne
   * Zakupy w internecie
   1. Użytkownicy powinni być podzieleni na grupy, dla których będą przygotowane indywidualne harmonogramy szkoleń oraz dedykowane kampanie phishingowe.
   2. Łączny czas trwania wszystkich materiałów szkoleniowych powinien wynosić co najmniej 8 godzin.
2. Dedykowaną platformę phishingową pozwalającą na generowanie i wysyłanie spreparowanych maili phishingowych do wszystkich użytkowników usługi oraz na generowanie, co najmniej, poniższych typów wiadomości e-mail:
   1. z linkiem prowadzącym do stronnym internetowej,
   2. z linkiem do portalu podszywającego się pod usługodawcę i pozwalającego na logowanie (weryfikację, czy użytkownicy są gotowi na fałszywej stronie portalu zalogować się swoim loginem i hasłem); platforma musi zapewniać bezpieczeństwo takiej operacji,
   3. z załącznikiem (szyfrowanym i niezaszyfrowanym) zawierającym potencjalnie niebezpieczny kod,
   4. z załącznikiem w postaci dokumentu Word lub Excel zawierającym potencjalnie niebezpieczny kod.

W przypadku, gdy użytkownik pozwoli się oszukać, platforma musi posiadać możliwość automatycznego skierowania takiego użytkownika na dodatkowe szkolenie lub ponowne wykonanie jednego z wcześniej ukończonych szkoleń.

1. dedykowaną platformę dostarczającą raporty obejmujące minimum:
   1. status wykonania szkoleń przez użytkowników, z podziałem na grupy i uwzględnieniem terminu wykonania szkoleń oraz wyniku quizów i testów,
   2. status kampanii, wraz z raportem o liczbie wysłanych e-maili oraz szczegółach zwierających informację: kto otworzył wiadomość, kto i kiedy pozwolił się oszukać, kto otworzył załącznik, jaka była platforma z jakiej wykonał tę akację oraz szczegółowe daty wykonania tych operacji.

**W ramach świadczonej usługi usługodawca musi**:

* + przygotować platformę do świadczenia usługi, założyć konta dla użytkowników oraz sprawdzić techniczne elementy związane z zapewnieniem dostarczenia wiadomości phishingowych z platformy do użytkowników,
  + - zaproponować do akceptacji Zamawiającego szczegółowy harmonogram szkoleń dopasowany do okresu świadczenia usługi,
  + - zaplanować na podstawie harmonogramu całą kampanię szkoleniową i dostarczyć ją użytkownikom za pośrednictwem dedykowanych wiadomości e-mail,
  + - dostarczać pełny raport z realizacji szkoleń dla użytkowników oraz przeprowadzonych kampanii po zakończeniu każdego modułu szkoleniowego oraz zbiorcze raporty końcowe,
  + - wprowadzić zmiany w harmonogramie i zakresie szkoleń w przypadku potrzeby modyfikacji, zmian kolejności szkoleń (2 zmiany miesięcznie) lub liczby użytkowników (nie więcej niż 10% zmian w okresie trwania usługi).

**Wymagania dodatkowe:**

Usługa ma być świadczona z centrum danych znajdującym się na terenie Unii Europejskiej. Dostawca platformy musi zapewnić całkowite usunięcie danych użytkowników po zakończeniu realizacji usługi. Wszystkie moduły (platforma szkoleniowa, platforma phishingowa i moduł raportowania) muszą pochodzić od jednego producenta.

Dla zapewnienia wysokiego poziomu usług, podmiot świadczący usługę musi posiadać certyfikat ISO 9001 w zakresie świadczenia usług. Zgłoszenia i komunikacja z usługodawcą będą przyjmowane w języku polskim w trybie 8x5, przez dedykowany portal serwisowy dostępny w sieci internet oraz infolinię w języku polskim 8x5. Czas reakcji usługodawcy nie może być dłuższy niż 1 godzina – reakcja w postaci połączenia telefonicznego lub odpowiedzi w portalu serwisowym.

1. Zawansowane Szkolenie z Cyberbezpieczeństwa dla kadry Zarządzającej kpl.1

**Cel szkolenia:**

Przekazanie menedżerom zaawansowanej wiedzy i narzędzi niezbędnych do efektywnej ochrony przed rosnącymi zagrożeniami cybernetycznymi, poprzez pogłębione rozumienie ryzyk, strategii obronnych, regulacji prawnych oraz najnowszych trendów w cyberbezpieczeństwie.

Wymogi dla osoby szkolącej:

Osoba musi posiadać stosowną wiedzę oraz minimum 2 letnie doświadczenia w przygotowywaniu i przeprowadzeniu szkoleń budujących i wzmacniających świadomość cyberzagrożeń.

Struktura programu szkoleniowego:

Szkolenie powinno być kompleksowym procesem, który umożliwia uczestnikom zdobycie dogłębnej wiedzy na temat wybranych zagadnień. Powinno ono nie tylko dostarczyć podstawowej informacji, ale także omówić zaawansowane aspekty danej tematyki, aby uczestnicy mieli pełniejsze zrozumienie tematu i byli w stanie zastosować zdobytą wiedzę w praktyce. Przekazywanie wiedzy powinno być interaktywne i angażujące, wykorzystując różnorodne metody nauczania, takie jak prezentacje, dyskusje, studia przypadków czy praktyczne ćwiczenia, co pozwoli uczestnikom efektywniej przyswoić omawiany materiał.

**W ramach przeprowadzonego szkolenia Wykonawca:**

1. Podstawowe informacje o obecnej sytuacji rynkowej powiązanej z tematyką cyberbezpieczeństwa:
2. Podstawy i definicje: zapewnienie uczestnikom solidnych podstaw w dziedzinie cyberbezpieczeństwa poprzez omówienie kluczowych pojęć i zasad. Ponadto, zostanie przedstawiona rola menedżera w formowaniu bezpiecznego środowiska cyfrowego, co pozwoli zrozumieć jak ważne jest aktywne zaangażowanie kierownictwa w procesy zapewnienia bezpieczeństwa informacji. W ten sposób uczestnicy będą mieć pełniejsze zrozumienie zarówno teoretycznych, jak i praktycznych aspektów cyberbezpieczeństwa oraz będą lepiej przygotowani do podejmowania decyzji w tym obszarze.
3. Statystyki i trendy: skoncentrowanie się na przekazaniu uczestnikom szczegółowej analizy globalnych i lokalnych danych dotyczących cyberataków. Poprzez omówienie ewolucji tych ataków oraz ich metodologii, uczestnicy zyskająwgląd w aktualne trendy i sposoby działania cyberprzestępców. Ponadto, zostaną przedstawione skutki, jakie cyberatakmoże mieć dla biznesu, co pozwoli uczestnikom lepiej zrozumieć znaczenie inwestycji w bezpieczeństwo informacji oraz skuteczne zarządzanie ryzykiem cybernetycznym dla organizacji. Dzięki temu będą mogli podejmować bardziej świadome decyzje w zakresie ochrony swoich danych i infrastruktury cyfrowej.
4. Omówienie światowych standardów i norm w zakresie cyberbezpieczeństwa i bezpieczeństwa informacji:
5. Normy ISO/IEC: Szczegółowe omówienie serii norm: ISO/IEC 27000: (zarysowuje leksykon oraz globalne zasady nadrzędne systemu zarządzania bezpieczeństwem informacji, kreśląc fundament pod szersze zrozumienie oraz efektywniejsze stosowanie pozostałych norm z rodziny 27000), ISO/IEC 27001 (stanowi kanon dotyczący wymagań dla systemów zarządzania bezpieczeństwem informacji, umożliwiając organizacjom zabezpieczenie informacji pod kątem ich poufności, integralności oraz dostępności przez implementację adekwatnych procedur zarządczych), ISO/IEC 27002 (oferuje referencyjny zbiór praktyk dla organizacji dążących do identyfikacji, wdrażania, utrzymania oraz doskonalenia swoich mechanizmów ochrony informacji w kontekście SZBI), ISO/IEC 27004 (dostarcza metodykę do monitorowania, przeglądu, oceny oraz doskonalenia efektywności systemu zarządzania bezpieczeństwem informacji, akcentując znaczenie mierzalnych wskaźników), ISO/IEC 27005 (zawiera wytyczne dotyczące zarządzania ryzykiem w kontekście bezpieczeństwa informacji, nakreślając proces identyfikacji, oceny oraz zarządzania ryzykiem informacyjnym), ISO/IEC 27006 (określa wymogi dla organizacji świadczących usługi certyfikacji systemów zarządzania bezpieczeństwem informacji, wyznaczając ramy dla procesu audytu i certyfikacji), ISO/IEC 27013 (podaje wytyczne integrujące system zarządzania bezpieczeństwem informacji z systemem zarządzania usługami IT, promując koherentną i efektywną infrastrukturę zarządzania), ISO/IEC 27017 (koncentruje się na bezpieczeństwie informacji w chmurze, proponując kontrole oraz wytyczne dla dostawców i użytkowników usług przetwarzania w chmurze), ISO/IEC 27018 (ustanawia kodeks praktyk dla ochrony informacji osobowych w chmurze, zgodnie z wymaganiami prywatności i ochrony danych), ISO/IEC 22301 (specyfikuje wymogi dla systemów zarządzania ciągłością działania, umożliwiając organizacjom przygotowanie na incydenty zakłócające normalne funkcjonowanie), ISO/IEC 24762 (zawiera wytyczne dla usług odzyskiwania po awariach w centrach danych i innych środowiskach IT, podkreślając kluczowe elementy potrzebne do przywrócenia operacji IT po katastrofie, ISO/IEC 27036 (skupia się na zarządzaniu bezpieczeństwem informacji w relacjach między organizacjami, oferując wytyczne dotyczące bezpieczeństwa w outsourcingu i partnerstwach biznesowych), ISO/IEC 31000 (dostarcza wytyczne dotyczące zarządzania ryzykiem ogólnym, promując model zarządzania ryzykiem, który można dostosować do różnych typów organizacji i kontekstów), 13501-2 (norma ta przeprowadza proces kategoryzacji reakcji na ogień wyrobów używanych w budownictwie oraz elementów konstrukcyjnych budowli, określając ich parametry odporności na pożary i zachowanie w ekstremalnych warunkach termicznych), norma 1627 (stanowi kryteria odporne na nieautoryzowany dostęp przez systemy zamykające, jak okna, drzwi oraz osłony, hierarchizując je zgodnie z ich zdolnością do stawiania oporu przy próbach sforsowania), norma 12209-04 (wytycza wymagania techniczne oraz procedury badawcze dla mechanizmów blokujących w obszarze budowlanym, takich jak zamki mechaniczne wraz z ich komponentami, oceniając ich funkcjonalność oraz niezawodność.), norma 50131-1 (określa specyfikacje dla systemów alarmowych przeznaczonych do sygnalizacji prób włamania czy napadu, wyznaczając standardy dotyczące ich skuteczności oraz metodyki testowania).
6. Omówienie znaczenia powyższych norm i ich w zapewnianiu wysokiego poziomu bezpieczeństwa informacji oraz praktycznego zastosowania w organizacjach.
7. Inne standardy: Przedstawienie i dyskusja na temat innych standardów:

* ramy dotyczące zarządzania ryzykiem cyberbezpieczeństwa - NIST Cybersecurity Framework;
* ramy dotyczące wdrażania, rozwoju i doskonalenia polityki IT – COBIT;
* zbiór praktyk dotyczący zarządzania usługami IT – ITIL;
* akceptowalna polityka szyfrowania SANS;
* techniki kryptograficzne - ENISA ;
* ramy ochrony informacji i zasobów federalnych agencji rządowych USA - 800-53 rev3.

1. Rola powyższych zagranicznych standardów w kształtowaniu efektywnych polityk bezpieczeństwa w organizacjach.
2. Omówienie zaawansowanych strategii ochrony organizacji:
3. Zarządzanie ryzykiem: Metody identyfikacji, oceny, mitygacji i monitorowania ryzyka cybernetycznego. Wykorzystanie narzędzi i technologii do analizy ryzyka.
4. Wprowadzenie do zarządzania incydentami, zdefiniowanie incydentów i wektorów ataku: atak przeprowadzony z nośnika wymiennego lub urządzenia peryferyjnego, atak wykorzystujący metody brute-force w celu złamania, degradacji lub zniszczenia systemów, sieci lub usług, ataki wykonane z poziomu witryny internetowej lub aplikacji internetowej, atak przeprowadzony za pośrednictwem wiadomości e-mail lub załącznika, naruszenia zasaddopuszczalnego użytkowania organizacji przez autoryzowanego użytkownika, z wyłączeniem powyższych kategorii, utrata lub kradzież urządzenia komputerowego lub nośnika używanego przez organizację, na przykład laptopa lub urządzenia typu smartfon.
5. Szczegółowy opis i kroki zarządzania incydentami:
6. wykrywanie: inicjacja procesu inicjującego, mającego na celu detekcję niestandardowych aktywności lub zdarzeń infrastrukturalnych, które mogą sygnalizować potencjalne zagrożenia w obszarze cybernetycznym;
7. rejestrowanie: operacja dokumentacyjna, polegająca na chronologicznym zapisie zaobserwowanych dysfunkcji w dedykowanych bazach danych, by zapewnić dokumentację dowodową dla późniejszych faz postępowania;
8. analizowanie: metodyczne badanie zgromadzonych artefaktów zdarzeń w celu zrozumienia ich genezy, dynamiki oraz wpływu na ekosystem informacyjny;
9. klasyfikowanie: systematyzacja incydentów według ustalonego kodu klasyfikacyjnego, uwzględniająca ich naturę, zasięg oraz potencjalne konsekwencje dla organizacji.
10. priorytetyzowanie: alokacja zasobów reakcyjnych na bazie oceny krytyczności, która koresponduje z możliwymi konsekwencjami incydentu dla misji instytucji;
11. podejmowanie działań naprawczych: inicjowanie interwencji korygujących mających na celu restytucję funkcji systemowych i prewencję przed podobnymi naruszeniami w przyszłości;
12. ograniczanie skutków incydentu: implementacja taktyk zaradczych, które mają za zadanie minimalizację negatywnych rezultatów incydentu oraz odbudowę stanu równowagi operacyjnej.
13. Priorytetyzacja incydentów na 3 kategorie: krytyczny, wysoki, średni na podstawie poniższych opisów:

* Priorytet krytyczny - Incydent wymaga niezwłocznego działania oraz zgłoszenia do właściwego CSIRT. Procesy wewnętrzne są sparaliżowane lub zakłócone w znaczącym stopniu. Istnieje wysokie ryzyko wycieku danych (np. danych osobowych) oraz utraty poufności, integralności i/lub dostępności informacji.
* Priorytet wysoki - Incydent wymaga szybkiego działania oraz zgłoszenia do właściwego CSIRT w ciągu 24 godzin. Procesy wewnętrzne są częściowo zakłócone lub sparaliżowane. Istnieje niskie ryzyko wycieku danych (np. danych osobowych) oraz utraty poufności, integralności i/lub dostępności informacji.
* Priorytet średni - Incydent prawdopodobnie nie wymaga niezwłocznego działania oraz zgłoszenia do właściwego CSIRT ze względu na brak symptomów działania z zewnątrz. Procesy wewnętrzne nie są sparaliżowane lub zakłócone w żadnym stopniu. Ryzyko wycieku danych (np. danych osobowych) oraz utraty poufności, integralności i/lub dostępności informacji nie występuje.

1. Budowanie zespołów ds. bezpieczeństwa: Definicja ról, odpowiedzialności, umiejętności oraz ścieżek rozwoju dla członków zespołu bezpieczeństwa.
2. Lista omówionych kompetencji w szkoleniu:

* Szef działu bezpieczeństwa (kierownik, dyrektor);
* Pełnomocnik ds. Bezpieczeństwa Informacji;
* Specjalista ds. Zarządzania Ryzykiem;
* Specjalista ds. Zgodności;
* Specjalista ds. Bezpieczeństwa Fizycznego;
* Architekt Systemów Bezpieczeństwa;
* Koordynator Programu Bezpieczeństwa;
* Analityk Bezpieczeństwa (II linia wsparcia);
* Inżynier ds. Bezpieczeństwa (II linia wsparcia);
* Administrator Systemów Bezpieczeństwa (II linia wsparcia);
* Specjalista ds. Odpowiedzi na Incydenty (III linia wsparcia);
* Specjalista ds. Testów Penetracyjnych (III linia wsparcia);
* Specjalista ds. Testów Socjotechnicznych (III linia wsparcia).

1. Regulacje prawne i compliance:
2. Zharmonizowanie działalności Podmiotu z imperatywami Ustawy o Krajowym Systemie Cyberbezpieczeństwa, z naciskiem na implementację procedur i protokołów zapewniających wytrzymałość infrastruktury informatycznej na potencjalne zagrożenia cyfrowe.- Inicjacja, adaptacja, perpetuacja oraz ewolucja Systemu Zarządzania Bezpieczeństwem Informacji, skonstruowanego na fundamencie czterech norm określonych w paragrafie 20 Krajowego Ramienia Interoperacyjności, stanowiących kamień węgielny dla ochrony danych.
3. Egzekwowanie procedury tworzenia redundancji danych dziennikowych poprzez generowanie kopii zapasowych, które będą przechowywane przez okres minimalny dwóch lat, zgodnie z dyrektywą zawartą w paragrafie 21 Krajowego Ramienia Interoperacyjności.
4. Implementacja kompleksowej agregacji logów (rejestrowanych zdarzeń) pochodzących z heterogenicznej gamy urządzeń, maszyn i aplikacji działających w ramach infrastruktury teleinformatycznej Podmiotu, umożliwiająca szczegółową analizę i audyt bezpieczeństwa.
5. Integracja z zaawansowanym systemem zarządzania cyberbezpieczeństwem S46 (S46-react), celem optymalizacji procesów detekcji, reagowania i prewencji w zakresie incydentów bezpieczeństwa cyfrowego.
6. - Kodyfikacja programu regularnych audytów wewnętrznych i zewnętrznych, obejmujących spektrum standardów i regulacji (KRI, KSC, ISO, RODO), wraz z przeprowadzaniem testów penetracyjnych i socjotechnicznych, mających na celu weryfikację skuteczności implementowanych środków ochrony.
7. Monitorowanie zdarzeń systemowych w trybie ciągłym, poprzez wykorzystanie mechanizmów korelacji zdarzeń, umożliwiających identyfikację i interpretację wzorców aktywności sugerujących potencjalne scenariusze ataków cybernetycznych.
8. Dostosowanie się do rozszerzonego zakresu wymagań wynikających z implementacji Dyrektywy NIS2, która wprowadza nowe, zaostrzone standardy w zakresie cyberbezpieczeństwa, wymagające od organizacji ponownej oceny i ulepszenia istniejących strategii ochrony danych.
9. Wyznaczenie dedykowanego Pełnomocnika ds. Systemu Zarządzania Bezpieczeństwem Informacji, którego rola nie będzie interferować ani generować konfliktów interesów z innymi kluczowymi funkcjami w organizacji (np. Inspektorem Ochrony Danych, Informatykiem, Dyrektorem).
10. Rekonfiguracja systemów informatycznych oraz protokołów pracy zdalnej w zgodzie ze zmienionymi standardami bezpieczeństwa, uwzględniającymi nowelizację Kodeksu Pracy, w celu zabezpieczenia integralności danych korporacyjnych w rozproszonym środowisku pracy.
11. Realizacja oczekiwań organów nadzorczych w kontekście konstruowania oraz utrzymywania zaawansowanych systemów cyberbezpieczeństwa, zdolnych do przeciwdziałania współczesnym zagrożeniom w przestrzeni cyfrowej.
12. Implementacja rygorystycznych protokołów ochrony danych osobowych, mających na celu eliminację ryzyka wycieków informacji, spowodowanych przez nieświadome bądź intencjonalne działania personelu organizacji.
13. Automatyzacja procesów aktualizacji oprogramowania w celu zapewnienia najwyższego poziom
14. Zarządzanie bezpieczeństwem w praktyce:
15. Zrozumienie znaczenia typów licencji względem konieczności ich testowania:

* Licencje niewyłączne, w których udzielający licencji może zezwolić na korzystanie z utworu wielu osobom równocześnie, które nie muszą mieć formy pisemnej.
* Licencje wyłączne, spotykane głównie w przypadku oprogramowania pisanego na zamówienie (np. strona www), w tym przypadku zwykle umowa licencyjna wynika z umowy o dzieło, na podstawie której firma wykonująca oprogramowanie wykonuje zamówioną aplikację, umowa taka wymaga formy pisemnej pod rygorem nieważności.
* Sublicencja, w której licencjobiorca może udzielić dalszej licencji, pod warunkiem wszakże takiego upoważnienia w jego umowie licencyjnej.
* OEM, to programy sprzedawane wraz ze sprzętem komputerowym (przypisane do konkretnego komputera), po wymianie sprzętu na nowszy, nie można ich przenieść na nowy komputer tylko trzeba ponownie je zakupić.
* BOX, to programy, które można przenosić na kolejne komputery jednak pod warunkiem, że zawsze zainstalowany jest tylko na jednym komputerze. Legalny jest tylko program ostatnio zainstalowany.
* Open Source (otwarte oprogramowanie) to alternatywa dla Freeware (wolne oprogramowanie), którego celem jest istnienie swobodnego dostępu do oprogramowania dla wszystkich jego uczestników. Zapewnia swoim użytkownikom prawo do legalnego oraz darmowe.

1. Techniki hardeningu: Wzmocnienie infrastruktury IT oraz zarządzanie patchami bezpieczeństwa.
2. Testy penetracyjne i socjotechniczne: Organizacja i przeprowadzanie testów w celu oceny gotowości organizacji

Szkolenie powinno odbyć się w miejscu wskazanym przez Zamawiającego w czasie nie krótszym niż 4 godziny robocze w ciągu jednego dnia z uwzględnieniem conajmniej 4 przerw po 15 minut. Powinno jest 30 minut na pytania i odpowiedzi uczestników.

1. Agregat prądotwórczy kontenerowy 75kVA szt.1

Parametry minimalne: dla UMiG Wodzisław

Agregat wykonany zgodnie z obowiązującymi normami i standardami

• 2006/42/CE Bezpieczeństwo maszyn.

Moc maksymalna agregatu w zakresie od 80 do 88 kVA

Moc znamionowa agregatu w zakresie od 75 do 80 kVA

cos fi – 0,8

Napięcie – 400/230 V

Częstotliwość – 50Hz

Agregat w wersji obudowanej, wyciszony. Stopień ochrony IP zgodnie z ISO 8528-13:2016

Wymagany jest centralny uchwyt załadunkowy

Zawiasy ze stali nierdzewnej, drzwi zamykane na klucz

Zewnętrzny przycisk zatrzymania awaryjnego

Amortyzatory drgań silnika i prądnicy

Osłona elementów gorących oraz wirujących

Agregat wymagany o wymiarach (d x sz x w.)

w zakresach d od 2200 do 2900 x sz od 850 do 1150 x w od 1300/ do 1750

oraz ciężarze własnym z płynami , bez paliwa w zakresach od 1200 do 1500 kg

Wyciszenie o bardzo wysokiej skuteczności, niepalne, z potwierdzeniem/atestem

Dopuszczalny poziom ciśnienia akustycznego z 7m. nie więcej niż – 90 dBA

Gwarancja min 2 lata

Wymagany silnik diesla

Wymagany jest zbiornik paliwa o pojemności w zakresach min od 120 do 260 litrów

Wlew paliwa na zewnątrz obudowy. Zamykany na zamek.

Silnik chłodzony cieczą

Prędkość obrotowa – 1500 r.p.m.

Układ elektryczny

Wyposażona w automatyczną regulację napięcia. Tolerancja napięcia +/-1%

Wymagana klasa IP - 23

Klasa izolacji – H

Paliwo Diesel

Zużycie paliwa w zakresie od 14 do 20 l/h (godz) przy obciążeniu 100%

Gwarancja min 2 lata

Regulator napięcia

UKŁADY SZR (SAMOCZYNNE ZAŁĄCZANIE REZERWY) w zabudowie obudowy agregatu wraz podłączeniem do

istniejącej instalacji od strony zasilania i odbioru oraz agregatu.

W okresie zimy przewidziane podgrzewanie. Należy przewidzieć grzejnik z płaszczem wodnym, gdy lokalna temperatura spada poniżej 4 stopni Celsjusza.

1. Agregat prądotwórczy kontenerowy 30kVA szt.1

Parametry minimalne: do referatu Gosp. Komunalnej

Agregat wykonany zgodnie z obowiązującymi normami i standardami

• 2006/42/CE Bezpieczeństwo maszyn.

Moc maksymalna agregatu w zakresie min 40 – 44kVA

Moc znamionowa agregatu w zakresie min 30– 32 kVA

cos fi – 0,8

Napięcie – 400/230 V

Częstotliwość – 50Hz

Agregat w wersji obudowanej, wyciszony. Stopień ochrony IP zgodnie z ISO 8528-13:2016

Wymagany jest centralny uchwyt załadunkowy

Zawiasy ze stali nierdzewnej, drzwi zamykane na klucz

Zewnętrzny przycisk zatrzymania awaryjnego

Amortyzatory drgań silnika i prądnicy

Osłona elementów gorących oraz wirujących

Projektowany agregat wymagany o wymiarach w zakresie (d x sz x w.) –

d 2200 do 2500 x sz 900 do 1600 x w 1200 do 1800 oraz ciężarze własnym z płynami , bez paliwa od 800 do 1200 kg

Dopuszczalny poziom ciśnienia akustycznego z 7m. nie więcej niż – 85 dBA

Wymagany silnik diesla

Wymagany jest zbiornik paliwa o pojemności w zakresie 90 do 160 litrów

Zużycie paliwa w zakresie od 8 do 10 l/h (godz) przy obciążeniu 100%

Wlew paliwa na zewnątrz obudowy. Zamykany na zamek.

Silnik chłodzony ciecz

Układ elektryczny

Akumulator rozruchowy

Układ SZR dla natężenia prądu 100A, aparaty wykonawcze stycznikowe, obudowa odporna na warunki atmosferyczne min IP65,

Wymagana klasa IP - 23

Klasa izolacji – H Gwarancja min 2 lata

Regulator napięcia

UKŁADY SZR (SAMOCZYNNE ZAŁĄCZANIE REZERWY) zabudowany w obudowie agregatu wraz podłączeniem do istniejącej instalacji od strony zasilania i odbioru oraz agregatu

W okresie zimy przewidziane podgrzewanie. Należy przewidzieć grzejnik z płaszczem wodnym, gdy lokalna temperatura powietrza spada poniżej 4 stopni Celsjusza.