Załącznik Nr 9 do SWZ

OPIS PRZEDMIOTU ZAMÓWIENIA

Znak postępowania: **IOŚ.271.1.14.2022**

Zamawiający:
Gmina Nowy Żmigród
ul. Mickiewicza 2
38-230 Nowy Żmigród

Nazwa zamówienia:
Dostawa sprzętu oraz oprogramowania w ramach projektu grantowego: Cyfrowa Gmina

Niniejszy dokument ma celu umożliwienie dokonania wyboru najkorzystniejszej oferty na dostawy, usługi teleinformatyczne, wykonanie modernizacji sieci LAN oraz realizację diagnozy cyberbezpieczeństwa, których podstawowym celem jest podniesienie poziomu cyfryzacji Urzędu oraz bezpieczeństwa teleinformatycznego (cyberbezpieczeństwa). Dokument zawiera opis wymagań pod kątem kryteriów funkcjonalnych, technicznych i jakościowych oraz wskazuje technologie, które powinny być wykorzystane tak, aby osiągnąć założone cele i zapewnić optymalną relację ceny do jakości rozwiązania. Opisane w dokumencie wymagania należy traktować jako podstawowe i minimalne, a te które zostały określone jako dodatkowe traktować należy jako nieobowiązkowe (fakultatywne).

Wymagania dotyczące sprzętu:

1. Dostarczony sprzęt musi być fabrycznie nowy (rok produkcji 2022), nieużywany, wolny od wad oraz wolny od obciążeń prawami osób trzecich. Oferowany sprzęt musi być objęty gwarancją producenta bądź gwarancją autoryzowanego serwisu producenta w Polsce i musi pochodzić z autoryzowanego kanału dystrybucji producenta przeznaczonego na teren Unii Europejskiej. Zamawiający nie dopuszcza dostawy urządzeń odnawianych, demonstracyjnych czy powystawowych. Wszystkie urządzenia muszą być dostarczone w oryginalnych opakowaniach producenta oraz powinny posiadać certyfikację oraz oznaczenie CE.
2. W celu uniknięcia błędów kompatybilności Zamawiający wymaga, aby wszystkie elementy oferowanych urządzeń oraz podzespoły montowane przez producenta były przez niego certyfikowane. **Wykonawca nie będący producentem oferowanego sprzętu nie może samodzielnie dokonywać jego modyfikacji. Zamawiający nie dopuszcza dostawy urządzeń modyfikowanych przez sprzedawcę oraz nie dopuszcza modyfikacji na linii produkcyjnej dystrybutorów lub innych dostawców.**
3. Dostarczany sprzęt powinien być kompletny i gotowy do uruchomienia, tak aby nie był konieczny zakup dodatkowych elementów wyposażenia lub dodatkowych akcesoriów.
4. Wykonawca dostarczy stosowne potwierdzenie gwarancji sprzętu i oprogramowania zapewniające, że sprzęt objęty jest gwarancją producenta.

Wymagania dotyczące oprogramowania:

1. Zamawiający informuje, że każde dostarczone oprogramowanie, licencje, systemy operacyjne muszą być opatrzone we wszystkie atrybuty oryginalności i legalności, wymagane przez producenta oprogramowania w zależności od dostarczanej wersji.
2. W ramach procedury odbioru, Zamawiający zastrzega sobie prawo do przeprowadzenia weryfikacji oryginalności i legalności dostarczonego oprogramowania bezpośrednio u producenta oprogramowania, przed podpisaniem protokołu odbioru w sposób, który uzna za nie budzący wątpliwości (bezsporny). W przypadku wykrycia, że zainstalowany system operacyjny lub inne dostarczone oprogramowanie jest nieoryginalne (nielegalne), nie jest nowe, było już używane lub było już wcześniej aktywowane, Zamawiający w takiej sytuacji odmówi przyjęcia dostarczonego oprogramowania i wezwie Wykonawcę do usunięcia nieprawidłowości w wyznaczonym terminie.

Wymagania dotyczące realizacji dostaw.

1. Wykonawca na swój koszt i ryzyko dostarczy przedmiot zamówienia, zgodny z wymaganiami przedstawionymi w niniejszym dokumencie.
2. Wykonawca w cenie oferty uwzględni wszystkie koszty niezbędne do realizacji dostawy, m.in. rozładunek, wniesienie oraz utrzymanie porządku w czasie rozładunku prowadzonego na terenie urzędu.
3. Wykonawca, co najmniej na 3 dni przed dniem planowanej dostawy sprzętu, dokona jej awizacji, to znaczy skontaktuje się z Zamawiającym w celu ustalenia miejsca i potwierdzenia konkretnego terminu dostawy.
4. Dostawa sprzętu odbędzie się w dniu roboczym, od poniedziałku do piątku, w godzinach 8:00 - 13:00, transportem zapewnionym przez Wykonawcę, na jego koszt i ryzyko wraz z wniesieniem do miejsca wskazanego przez Zamawiającego.
5. Do czasu odbioru sprzętu przez Zamawiającego, ryzyko wszelkich niebezpieczeństw związanych z jego ewentualnym uszkodzeniem lub utratą ponosi Wykonawca.
6. Wraz ze sprzętem Wykonawca zobowiązany jest przekazać Zamawiającemu listę numerów seryjnych dostarczonych urządzeń wszelką dokumentację dostarczoną przez producenta sprzętu.

Pozostałe wymagania stawiane Wykonawcom.

Poza dostawami i usługami podstawowymi, Wykonawca jest zobowiązany do skalkulowania wszelkich usług pomocniczych, jakie uzna za niezbędne do prawidłowego wykonania przedmiotu zamówienia dla przyjętej technologii, uwzględniając warunki ich wykonania, ze szczególnym uwzględnieniem zakresu odnoszącego się do modernizacji sieci LAN. Wykonawca powinien uwzględnić w cenie w ramach kosztów dodatkowych:

1. koszty zabezpieczenia istniejących elementów obiektu oraz wyposażenia (urządzeń) Zamawiajacego przed ich zniszczeniem w trakcie wykonywania prac;
2. koszty związane z zorganizowaniem pracy w sposób minimalizujący zakłócenie prowadzenia bieżącej działalności Zamawiającego;
3. koszty zapewnienia bezpieczeństwa bhp i ppoż. w trakcie realizacji prac;

4. koszty testów, prób, badań, odbiorów technicznych - jeśli są wymagane.

Stosowanie rozwiązań z zakresu interoperacyjności

Podmioty realizujące zadania publiczne zobowiązane są do stosowania rozwiązań z zakresu interoperacyjności m.in. na poziomie technologicznym. Interoperacyjność osiąga się poprzez stosowania minimalnych wymagań dla systemów teleinformatycznych. Zgodnie z §20 ust. 2 pkt. 12 Rozporządzenia Rady Ministrów w sprawie Krajowych Ram Interoperacyjności (KRI) zapewnienie odpowiedniego poziomu bezpieczeństwa w systemach teleinformatycznych polega m.in. na:

1. zgodności systemów teleinformatycznych z odpowiednimi normami i politykami bezpieczeństwa,
2. redukcji ryzyk wynikających z wykorzystania opublikowanych podatności technicznych systemów teleinformatycznych,
3. zapewnienia bezpieczeństwa plików,
4. dbałość o aktualizację oprogramowania.

Dodatkowym ważnym elementem systemu jest możliwość rejestrowania i przechowywania zapisów w dziennikach systemowych (logowanie zdarzeń). Konieczność zapewnienia tej funkcjonalności wynika z:

1. §21 ust. 1 KRI (zapewnienie rozliczalności w systemach teleinformatycznych w postaci elektronicznej)
2. Art. 22 i 23 Ustawy z dnia 5 lipca 2018 o Krajowym Systemie Cyberbezpieczeństwa

Wdrożone rozwiązania powinny spełniać wymagania przywołanych aktów prawnych oraz standardów rynkowych.

Dokumenty odbioru końcowego:

1. Protokoły odbiorów częściowych.
2. Protokoły z pomiarów i testów (jeśli dotyczy).
3. Odpowiednie atesty i certyfikaty (jeśli są wymagane).
4. Instrukcje obsługi, dokumentacje i inne dokumenty dostarczane wraz ze sprzętem, przez producenta.

Zamawiający wymaga zaoferowania urządzeń, sprzętu, dostaw oraz usług spełniających wymagania techniczne, eksploatacyjne, funkcjonalne oraz jakościowe określone w niniejszym dokumencie, natomiast realizacja całego zakresu zamówienia musi być wykonana w oparciu o obowiązujące przepisy, przez Wykonawcę posiadającego stosowne doświadczenie, uprawnienia i potencjał wykonawczy oraz osoby o odpowiednich kwalifikacjach i doświadczeniu zawodowym.

1. STACJE ROBOCZE

ATRYBUT	MINIMALNE WYMAGANIA FUNKCJONALNE, TECHNICZNE, UŻYTKOWE, JAKOŚCIOWE
Ilość	7 zestawów
Określenie oferowanej konfiguracji	Zamawiający wymaga określenia przez oferenta w formularzu ofertowym co najmniej następujących cech oferowanego rozwiązania: producent (marka), model (symbol), rodzaj obudowy, procesor, pamięć operacyjna, pamięć masowa, system operacyjny, gwarancja
Obudowa	Małogabarytowa typu SFF przystosowana na etapie produkcji do pracy w pozycji pionowej i poziomej, wyposażona przynajmniej w: ▪ 1 zewnętrzną zatokę 5.25" ▪ 1 zewnętrzną zatokę 3,5” ▪ 1 wewnętrzną zatokę 3,5” ▪ Beznarzędziowe otwieranie i zamykanie ▪ Beznarzędziowy montaż napędów, dysków i kart rozszerzeń ▪ Złącze Kensigton Lock Wymagana możliwość otwarcia obudowy komputera i dołożenia komponentów przez wykwalifikowany personel Zamawiającego bez utraty gwarancji.
Zasilacz	O mocy minimalnej 300W i sprawności 80+ Bronze
Procesor	Wymagany procesor klasy x86 wielordzeniowy, umożliwiający osiągnięcie w teście Passmark CPU Mark, w kategorii Average CPU Mark wyniku min. 12.000 punktów. **Dokumentem potwierdzającym spełnienie wymagań będzie złożony przez Wykonawcę wydruk ze strony www.cpubenchmark.net**
Płyta główna	Płyta główna wyposażona fabrycznie w następujące złącza i gniazda: min. jedno gniazdo PCI-Ex16, min. jedno gniazdo PCI-E x1 min. 10x USB min. 4x SATA III min. 1x M.2 slot (Key M) z obsługą dysków PCIe x4 i/lub SATA 6Gb/s 2260/2280
BIOS	Zgodny ze specyfikacją UEFI
Pamięć operacyjna	Min. 16 GB z możliwością rozbudowy do 64GB
Pamięć masowa	Min. 512GB SSD
Napęd optyczny	Nagrywarka DVD+/-RW
Porty w tylnej części komputera	Komputer wyposażony w następujące gniazda na tylnym panelu I/O: ▪ co najmniej 4 gniazda USB 2.0; ▪ co najmniej 2 gniazda USB 3.2 ▪ 1 gniazdo portu LAN RJ-45;

	▪ gniazda video HDMI, D-Sub ▪ Zestaw gniazd audio wielokanałowej karty dźwiękowej;
Porty w przedniej części komputera	Komputer wyposażony w następujące gniazda na przednim panelu obudowy ▪ 2 gniazda USB 3.2 i min 2 gniazda USB 2.0 ▪ 1 gniazdo do przyłączenia słuchawek i 1 gniazdo do przyłączenia mikrofonu (dopuszcza się złącze współdzielone);
Komunikacja	Karta sieciowa 10/100/1000Mb/s
Bezpieczeństwo	▪ Możliwość zastosowania mechanicznego zabezpieczenia przed kradzieżą komputera. ▪ Możliwość zastosowania mechanicznego zabezpieczenia przed niepowołanym dostępem do wnętrza obudowy.
Peryferia	Przewodowa klawiatura i mysz
System operacyjny	Bezterminowa licencja oprogramowania systemu operacyjnego klasy Microsoft Windows 11 Professional lub równoważny. Za równoważny system operacyjny Zamawiający uzna system spełniający następujące minimalne parametry: 1. Możliwość dokonywania aktualizacji i poprawek systemu przez Internet; 2. Możliwość dokonywania uaktualnień sterowników urządzeń przez Internet – witrynę producenta systemu; 3. Darmowe aktualizacje w ramach wersji systemu operacyjnego przez Internet (niezbędne aktualizacje, poprawki, biuletyny bezpieczeństwa muszą być dostarczane bez dodatkowych opłat) – wymagane podanie nazwy strony serwera WWW; 4. Internetowa aktualizacja zapewniona w języku polskim; 5. Wbudowana zapora internetowa (firewall) dla ochrony połączeń internetowych; 6. Zintegrowana z systemem konsola do zarządzania ustawieniami zapory i regułami IPSec v4 i v6; 7. Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, przeglądarka internetowa, pomoc, komunikaty systemowe; 8. Wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (np.: drukarek, urządzeń sieciowych, standardów USB, Plug&Play, Wi-Fi); 9. Możliwość zdalnej automatycznej instalacji, konfiguracji, administrowania oraz aktualizowania systemu; 10. Zabezpieczony hasłem hierarchiczny dostęp do systemu, konta i profile użytkowników zarządzane zdalnie; 11. Praca systemu w trybie ochrony kont użytkowników;

	12. Zintegrowany z systemem moduł wyszukiwania informacji (plików różnego typu) dostępny z kilku poziomów: poziom menu, poziom otwartego okna systemu operacyjnego; 13. System wyszukiwania oparty na konfigurowalnym przez użytkownika module indeksacji zasobów lokalnych; 14. Zintegrowane z systemem operacyjnym narzędzia zwalczające złośliwe oprogramowanie; 15. Aktualizacje dostępne u producenta nieodpłatnie bez ograniczeń czasowych; 16. Wbudowany system pomocy w języku polskim; 17. System operacyjny powinien być wyposażony w możliwość przystosowania stanowiska dla osób niepełnosprawnych (np. słabo widzących); 18. Możliwość zarządzania stacją roboczą poprzez polityki – przez politykę rozumiemy zestaw reguł definiujących lub ograniczających funkcjonalność systemu lub aplikacji; 19. System posiadać powinien narzędzia służące do administracji, do wykonywania kopii zapasowych polityk i ich odtwarzania oraz generowania raportów z ustawień polityk; 20. Zdalna pomoc i współdzielenie aplikacji – możliwość zdalnego przejęcia sesji zalogowanego użytkownika celem rozwiązania problemu z komputerem; 21. Graficzne środowisko instalacji i konfiguracji; 22. Zarządzanie kontami użytkowników sieci oraz urządzeniami sieciowymi tj. drukarki, modemy, woluminy dyskowe, usługi katalogowe; 23. Możliwość przywracania plików systemowych; 24. Możliwość „downgrade” do niższej wersji. System musi być nowy (nie aktywowany wcześniej na innym urządzeniu), zainstalowany fabrycznie na dostarczonym komputerze przez producenta sprzętu.
Certyfikaty i normy	1. Spełnianie normy ISO 9001 lub równoważnej dla producenta sprzętu w zakresie projektowania i produkcji - dokumentem potwierdzającym spełnienie wymagań będzie załączony do oferty certyfikat producenta. 2. Spełnienie normy ISO 14001 lub równoważnej dla producenta sprzętu w zakresie projektowania i produkcji - dokumentem potwierdzającym spełnienie wymagań będzie załączony do oferty certyfikat producenta. 3. Spełnienie normy SA 8000:2014 lub równoważnej przez producenta sprzętu w zakresie projektowania i produkcji - dokumentem potwierdzającym spełnienie wymagań będzie załączony do oferty certyfikat producenta

	4. Oferowany sprzęt musi posiadać certyfikację oraz oznaczenie CE
Warunki gwarancyjno-serwisowe	Dla zaoferowanej stacji roboczej Zamawiający wymaga następujących warunków gwarancji i serwisu: 1. Minimalny czas trwania gwarancji udzielonej przez producenta na stację roboczą wynosi 24 miesiące. 2. W przypadku awarii dysku twardego (w urządzeniu objętym aktywnym wparciem technicznym) powodującej konieczność jego wymiany, uszkodzony dysk pozostaje u Zamawiającego. 3. Okres zabezpieczenia serwisowego na dyski twarde, o którym mowa w pkt 2 musi odpowiadać okresowi udzielonej gwarancji na sprzęt. 4. Wymagany czas reakcji serwisu na zgłoszenie - do końca następnego dnia roboczego. 5. Wymagana możliwość ściągnięcia aktualnych sterowników z witryny producenta komputera poprzez podanie numeru seryjnego komputera.
Dodatkowy okres gwarancji (wymaganie fakultatywne)	Zaoferowanie stacji roboczej z dodatkową gwarancją producenta wydłużającą gwarancję podstawową o okres dodatkowych 12 lub więcej miesięcy jest wymogiem nieobowiązkowym (fakultatywnym) i jest kryterium dodatkowo punktowanym zgodnie z kryterium oceny ofert dla Kryterium „gwarancja stacji roboczych (KG1)” **Potwierdzenie spełnienia tego kryterium Wykonawca zaznacza w formularzu ofertowym.**

2. LICENCJA NA PAKIET OPROGRAMOWANIA BIUROWEGO

MINIMALNE WYMAGANIA FUNKCJONALNE, TECHNICZNE, UŻYTKOWE, JAKOŚCIOWE
Wymagana jest dostawa oprogramowania służącego do typowych zastosowań biurowych, takich jak edycja tekstu, wykonywanie obliczeń rachunkowo/księgowych, tworzenie i obsługa prezentacji, które mają zostać dostarczone jako jeden zintegrowany produkt. Zamawiający wymaga określenia przez oferenta w formularzu ofertowym co najmniej następujących cech oferowanego oprogramowania: producent (marka), model (symbol), wersji, typ licencji oraz liczba licencji. Zamawiający wymaga dostawy w najnowszej dostępnej na rynku wersji, w formie licencji bezterminowej dla 9 (dziewięciu) stacji roboczych oprogramowania biurowego klasy Microsoft Office lub równoważny. Za równoważny pakiet biurowy Zamawiający uzna oprogramowanie spełniające następujące minimalne wymagania poprzez wbudowane mechanizmy, bez użycia dodatkowych aplikacji: 1. wymagania odnośnie interfejsu użytkownika:

- pełna polska wersja językowa interfejsu użytkownika,
- prostota i intuicyjność obsługi, pozwalająca na pracę osobom nieposiadającym umiejętności technicznych;

2. oprogramowanie musi umożliwiać tworzenie i edycję dokumentów elektronicznych w ustalonym formacie, który spełnia następujące warunki:
   - posiada kompletny i publicznie dostępny opis formatu,
   - ma zdefiniowany układ informacji w postaci XML zgodnie z Załącznikiem 2 Rozporządzenia Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (Dz. U. 2012, poz. 526);
3. oprogramowanie musi umożliwiać dostosowanie dokumentów i szablonów do potrzeb instytucji;
4. w skład oprogramowania muszą wchodzić narzędzia programistyczne umożliwiające automatyzację pracy i wymianę danych pomiędzy dokumentami i aplikacjami (język makropoleceń, język skryptowy);
5. do aplikacji musi być dostępna pełna dokumentacja w języku polskim;

Pakiet zintegrowanych aplikacji biurowych musi zawierać:

1. Edytor tekstów,
2. Arkusz kalkulacyjny,
3. Narzędzie do przygotowywania i prowadzenia prezentacji,
4. Narzędzie do zarządzania informacją prywatną (pocztą elektroniczną, kalendarzem, kontaktami i zadaniami).

Edytor tekstów musi umożliwiać:

a) edycję i formatowanie tekstu w języku polskim wraz z obsługą języka polskiego w zakresie sprawdzania pisowni i poprawności gramatycznej oraz funkcjonalnością słownika wyrazów bliskoznacznych i autokorekty,
b) wstawianie oraz formatowanie tabel,
c) wstawianie oraz formatowanie obiektów graficznych,
d) wstawianie wykresów i tabel z arkusza kalkulacyjnego (wliczając tabele przestawne),
e) automatyczne numerowanie rozdziałów, punktów, akapitów, tabel i rysunków,
f) automatyczne tworzenie spisów treści,
g) formatowanie nagłówków i stopek stron,
h) śledzenie i porównywanie zmian wprowadzonych przez użytkowników w dokumencie,
i) nagrywanie, tworzenie i edycję makr automatyzujących wykonywanie czynności,
j) określenie układu strony (pionowa/pozioma),
k) wydruk dokumentów,
l) wykonywanie korespondencji seryjnej bazując na danych adresowych pochodzących z arkusza kalkulacyjnego i z narzędzia do zarządzania informacją prywatną,

m) pracę na dokumentach utworzonych przy pomocy posiadanego przez Zamawiającego oprogramowania Microsoft Word 2003 lub Microsoft Word 2007, 2010 i 2013 z zapewnieniem bezproblemowej konwersji wszystkich elementów i atrybutów dokumentu,
n) zabezpieczenie dokumentów hasłem przed odczytem oraz przed wprowadzaniem modyfikacji,
o) wymagana jest dostępność do oferowanego edytora tekstu bezpłatnych narzędzi umożliwiających wykorzystanie go, jako środowiska kreowania aktów normatywnych i prawnych, zgodnie z obowiązującym prawem,
p) wymagana jest dostępność do oferowanego edytora tekstu bezpłatnych narzędzi umożliwiających podpisanie podpisem elektronicznym pliku z zapisanym dokumentem przy pomocy certyfikatu kwalifikowanego zgodnie z wymaganiami obowiązującego w Polsce prawa;

Arkusz kalkulacyjny musi umożliwiać:
a) tworzenie raportów tabelarycznych,
b) tworzenie wykresów liniowych (wraz linią trendu), słupkowych, kołowych,
c) tworzenie arkuszy kalkulacyjnych zawierających teksty, dane liczbowe oraz formuły przeprowadzające operacje matematyczne, logiczne, tekstowe, statystyczne oraz operacje na danych finansowych i na miarach czasu,
d) tworzenie raportów z zewnętrznych źródeł danych (inne arkusze kalkulacyjne, bazy danych zgodne z ODBC, pliki tekstowe, pliki XML, WebService),
e) obsługę kostek OLAP oraz tworzenie i edycję kwerend bazodanowych i webowych. Narzędzia wspomagające analizę statystyczną i finansową, analizę wariantową i rozwiązywanie problemów optymalizacyjnych,
f) tworzenie raportów tabeli przestawnych umożliwiających dynamiczną zmianę wymiarów oraz wykresów bazujących na danych z tabeli przestawnych,
g) wyszukiwanie i zamianę danych,
h) wykonywanie analiz danych przy użyciu formatowania warunkowego,
i) nazywanie komórek arkusza i odwoływanie się w formułach po takiej nazwie,
j) nagrywanie, tworzenie i edycję makr automatyzujących wykonywanie czynności,
k) formatowanie czasu, daty i wartości finansowych z polskim formatem,
l) zapis wielu arkuszy kalkulacyjnych w jednym pliku,
m) zachowanie pełnej zgodności z formatami plików utworzonych za pomocą posiadanego przez Zamawiającego oprogramowania Microsoft Excel 2003 oraz Microsoft Excel 2007, 2010 i 2013, z uwzględnieniem poprawnej realizacji użytych w nich funkcji specjalnych i makropoleceń,
n) zabezpieczenie dokumentów hasłem przed odczytem oraz przed wprowadzaniem modyfikacji;

Narzędzie do przygotowywania i prowadzenia prezentacji musi umożliwiać:
a) przygotowywanie prezentacji multimedialnych,
b) prezentowanie przy użyciu projektora multimedialnego,
c) drukowanie w formacie umożliwiającym robienie notatek,
d) zapisanie jako prezentacja tylko do odczytu,

e) nagrywanie narracji i dołączanie jej do prezentacji,
f) opatrywanie slajdów notatkami dla prezentera,
g) umieszczanie i formatowanie tekstów, obiektów graficznych, tabel, nagrań dźwiękowych i wideo,
h) umieszczanie tabel i wykresów pochodzących z arkusza kalkulacyjnego,
i) odświeżenie wykresu znajdującego się w prezentacji po zmianie danych w źródłowym arkuszu kalkulacyjnym,
j) możliwość tworzenia animacji obiektów i całych slajdów,
k) prowadzenie prezentacji w trybie prezentera, gdzie slajdy są widoczne na jednym monitorze lub projektorze, a na drugim widoczne są slajdy i notatki prezentera,
l) pełna zgodność z formatami plików utworzonych za pomocą posiadanego przez Zamawiającego oprogramowania MS PowerPoint

Narzędzie do zarządzania informacją prywatną (pocztą elektroniczną, kalendarzem, kontaktami i zadaniami) musi umożliwiać:
a) pobieranie i wysyłanie poczty elektronicznej z serwera pocztowego,
b) przechowywanie wiadomości na serwerze lub w lokalnym pliku tworzonym z zastosowaniem efektywnej kompresji danych,
c) filtrowanie niechcianej poczty elektronicznej (SPAM) oraz określanie listy zablokowanych i bezpiecznych nadawców,
d) tworzenie katalogów, pozwalających katalogować pocztę elektroniczną,
e) automatyczne grupowanie poczty o tym samym tytule,
f) tworzenie reguł przenoszących automatycznie nową pocztę elektroniczną do określonych katalogów bazując na słowach zawartych w tytule, adresie nadawcy i odbiorcy,
g) oflagowanie poczty elektronicznej z określeniem terminu przypomnienia, oddzielnie dla nadawcy i adresatów,
h) mechanizm ustalania liczby wiadomości, które mają być synchronizowane lokalnie,
i) zarządzanie kalendarzem,
j) udostępnianie kalendarza innym użytkownikom z możliwością określania uprawnień użytkowników,
k) przeglądanie kalendarza innych użytkowników,
l) zapraszanie uczestników na spotkanie, co po ich akceptacji powoduje automatyczne wprowadzenie spotkania w ich kalendarzach,
m) zarządzanie listą zadań,
n) zlecanie zadań innym użytkownikom,
o) zarządzanie listą kontaktów, p) udostępnianie listy kontaktów innym użytkownikom,
p) przeglądanie listy kontaktów innych użytkowników,
q) możliwość przesyłania kontaktów innym użytkowników

3. SZAFA TELEINFORMATYCZNA RACK 42U Z WYPOSAŻENIEM

ATRYBUT	MINIMALNE WYMAGANIA FUNKCJONALNE, TECHNICZNE, UŻYTKOWE, JAKOŚCIOWE
Ilość	1 zestaw
Określenie oferowanej konfiguracji	Zamawiający wymaga określenia przez oferenta w formularzu ofertowym co najmniej następujących cech oferowanego rozwiązania: producent (marka), model (symbol).
Cechy fizyczne	Obciążalność min. 1000 kg Możliwość montażu urządzeń o sumarycznej wysokości 42U Wymiary szafy: min. 800mmx1000mmx2055mm (szerokość/głębokość/wysokość) Wyposażona w 4 stopki z regulacją wysokości
Konstrukcja	Grubość materiału: Rama, góra, dół, przednie drzwi, tylne drzwi, boczne drzwi: min. 1,2 mm Szyny poziome: min. 1,5 mm Szyny pionowe: min. 2,0 mm
Drzwi	Drzwi przednie przeszklone (z wklejoną szybą hartowaną) z wentylowanymi bokami, wyposażone w zamek. Drzwi tylne stalowe perforowane, wentylowane, wyposażone w zamek. Zdejmowane panele boczne.
Stopień ochrony	Co najmniej IP20
Wyposażenie	Półka rackowa uniwersalna, wysokość montażowa max 1U, głębokość min. 270mm, mocowanie czteropunktowe doczołowe - min. 1 sztuka Panel wentylatorów wymuszający obieg powietrza wewnątrz szafy pomiędzy urządzeniami. Wymagany wbudowany termostat pozwalający oszczędzać energię wyłączając wentylatory po osiągnięciu optymalnej temperatury.Wysokość montażowa max 1U, Szerokość 19'', Montaż do szyn pionowych szafy, Wbudowany czujnik temperatury, Wbudowany kabel zasilający, Wbudowane 4 wentylatory Listwa zasilająca do zasilania wszystkich urządzeń podłączonych do zasilania awaryjnego (UPS). Wysokość montażowa max 1U, Uchwyty metalowe do montażu w szafie 19" , Możliwość montażu podłoża/ściany, 9 gniazd 230V PL (10A) z uziemieniem, przewód min. 3m Poziomy organizer kabli, wysokość montażowa max 1U, montaż doczołowy do szyn Rack - min. 1 sztuka Szafa wyposażona w zestaw śrub, podkładek, koszyków przystosowanych do montażu wewnątrz szafy pozwalający na montaż wszystkich akcesoriów

	takich jak: patch panele, listwy zasilające, półki do pionowych szyn w każdej szafie rack w ilości wymaganej przez zamontowane urządzenia.
Warunki gwarancyjno-serwisowe	Gwarancja produecnta min. 2 lata (24 miesiące)

4. ZASILACZ AWARYJNY UPS ONLINE

ATRYBUT	MINIMALNE WYMAGANIA FUNKCJONALNE, TECHNICZNE, UŻYTKOWE, JAKOŚCIOWE
Ilość	1 sztuka
Określenie oferowanej konfiguracji	Zamawiający wymaga określenia przez oferenta w formularzu ofertowym co najmniej następujących cech oferowanego zasilacza: producent (marka), model (symbol), moc, gwarancja
Obudowa	▪ Wysokość obudowy max 2U - w komplecie szyny zapewniające montaż zasilacza w szafie Rack 19’’ ▪ Wyposażona w panel kontrolny LCD, który ma w czytelny sposób informować o trybie pracy, parametrach zasilacza, pozostałej autonomii pracy z baterii, umożliwiać konfigurację parametrów oraz pozwalać na diagnostykę zasilacza.
Technologia	True ON LINE Double Conversion
Moc	2700W (3000VA)
Wejściowy współczynnik mocy	≥0,99
Sprawność w trybie On-Line	>92%
Rodzaj i ilość gniazd	▪ Min. IEC320-C13 x8 ▪ Min. IEC320-C19 x1
Start z baterii (tzw. zimny start)	TAK - ma zapewnić możliwość uruchomienie zasilacza nawet w przypadku całkowitego braku napięcia zasilającego.
Czas podtrzymania	Wymagany jest następujący czas podtrzymania zasilania realizowany za pomocą oferowanych baterii wewnętrznych dla następujących obciążeń zasilacza (wg danych z karty katalogowej producenta): ▪ przy 50% obciążeniu nie mniej niż 12 minut ▪ przy 75% obciążeniu nie mniej niż 7 minut
Cykl ładowania	Wg DIN 41773 z automatycznym wyłączeniem ładowania wg kryterium prądu i napięcia, z kontrolą czasu.
Komunikacja	RS232, USB, TVSS, SNMP Slot, złącze REPO
Pozostałe wymagania	▪ Automatyczna diagnostyka gwarantująca pełną sprawność urządzenia, kontrolę podzespołów i parametrów pracy bez konieczności ingerencji użytkownika.

	▪ Odporność na przeciążenia przy występowaniu stanów nieustalonych i wysoka tolerancja na błędy obsługi.
Normy, certyfikaty i standardy	▪ Oferowany sprzęt musi posiadać certyfikację oraz oznaczenie CE. ▪ Wymagane spełnienie norm w zakresie bezpieczeństwa: EN 62040-1:2008 + A1:2013, EN 62040-3 :2001, EN 60950-1, EN61000-3-2:2014
Oprogramowanie	W komplecie z serwerem wymagane jest dostarczenie oprogramowania, które można skonfigurować w taki sposób aby wyłączyło serwer gdy baterie będą na wyczerpaniu.
Gwarancja producenta	Co najmniej 2 lata (24 miesiące)

5. SERWER

ATRYBUT	MINIMALNE WYMAGANIA FUNKCJONALNE, TECHNICZNE, UŻYTKOWE, JAKOŚCIOWE
Ilość	1 zestaw
Określenie oferowanej konfiguracji	Zamawiający wymaga określenia przez oferenta w formularzu ofertowym co najmniej następujących cech oferowanego rozwiązania: producent (marka), model, rodzaj obudowy, procesor, pamięć, kontroler Raid, karta zarządzania, licencje na system operacyjny, gwarancja
Obudowa	Obudowa Rack o wysokości max 1U z możliwością instalacji min. 8 dysków wraz z kompletem wysuwanych szyn umożliwiających montaż w szafie Rack i wysuwanie serwera do celów serwisowych oraz organizerem do kabli. Na potrzeby przyszłej rozbudowy wymagana jest obudowa z możliwością wyposażania w kartę umożliwiającą dostęp bezpośredni poprzez urządzenia mobilne - serwer musi posiadać możliwość konfiguracji oraz monitoringu najważniejszych komponentów serwera przy użyciu dedykowanej aplikacji mobilnej min. (Android/ Apple iOS) przy użyciu jednego z protokołów BLE/ WIFI.
Płyta główna	Na potrzeby przyszłej rozbudowy wymagana jest płyta główna z możliwością zainstalowania dwóch procesorów, wyposażona w minimum 16 slotów przeznaczonych do instalacji pamięci, z możliwością obsługi 1TB pamięci RAM.
Wydajność	Serwer z zainstalowanymi dwoma procesorami, klasy x86 dedykowanymi do pracy z zaoferowanym serwerem umożliwiającymi osiągnięcie w teście SPECrate®2017_int_base wyniku co najmniej 125 punktów przeprowadzonego dla konfiguracji dwuprocesorowej. **Dokumentem potwierdzającym spełnienie wymagań będzie załączony do oferty raport z testu wydajności SPECrate®2017_int_base**

	opublikowany na stronie www.spec.org dla oferowanego modelu serwera z oferowanym modelem procesora.
Pamięć operacyjna	Co najmniej 192 GB RAM
Funkcjonalność pamięci RAM	Advanced ECC, Memory Page Retire, Fault Resilient Memory, Memory Self-Healing lub PPR, Partial Cache Line Sparing
Gniazda PCI	Co najmniej jeden slot PCIe x16 generacji 4
Interfejsy sieciowe	2 interfejsy sieciowe 1GbE w standardzie BaseT 2 interfejsy sieciowe 10GbE w standardzie SFP+
Pamięć masowa (dyski)	1) Serwer musi mieć możliwość instalacji dysków SAS, SATA, SSD 2) Zainstalowane 5 dysków SSD o pojemności min. 1.9TB, 6Gb, Hot-Plug. 3) Zainstalowane 2 dyski M.2 o pojemności 240GB z możliwością konfiguracji RAID 1. 4) Na potrzeby przyszłej rozbudowy musi zostać zapewniona możliwość zainstalowania dedykowanego modułu dla hypervisora wirtualizacyjnego, wyposażonego w 2 nośniki typu flash o pojemności min. 64GB, z możliwością konfiguracji zabezpieczenia synchronizacji pomiędzy nośnikami z poziomu BIOS serwera - rozwiązanie nie może powodować zmniejszenia ilości wnęk na dyski twarde.
Kontroler RAID	Sprzętowy kontroler dyskowy posiadający min. 4GB nieulotnej pamięci cache, umożliwiający konfigurację co najmniej następujących poziomów RAID: 0, 1, 5, 6, 10, 50, 60. Wymagane wsparcie dla dysków SED.
Video	Zintegrowana karta graficzna umożliwiająca wyświetlenie rozdzielczości min. 1600x900
Wentylatory	Redundantne
Zasilacze	Redundantne, Hot-Plug o mocy min. 800W.
Bezpieczeństwo	▪ W celu ochrony przed nieautoryzowanym dostępem do dysków twardych wymagany jest zatrzask górnej pokrywy oraz blokada na ramce panela zamykana na klucz. ▪ Możliwość wyłączenia w BIOS funkcji przycisku zasilania. ▪ BIOS musi mieć możliwość przejścia do bezpiecznego trybu rozruchowego z możliwością zarządzania blokadą zasilania, panelem sterowania oraz zmianą hasła. ▪ Wymagany wbudowany czujnik otwarcia obudowy współpracujący z BIOS i kartą zarządzającą. ▪ Wymagany moduł TPM 2.0 pełniący funkcję dodatkowej warstwy sprzętowej do obsługi różnych działań kryptograficznych, w tym do ochrony kluczy szyfrowania, danych uwierzytelniania i innych wrażliwych danych. ▪ Musi istnieć możliwość dynamicznego włączania i wyłączania portów USB na obudowie bez potrzeby restartu serwera.

	▪ Musi istnieć możliwość wymazania danych ze znajdujących się dysków wewnątrz serwera niezależne od zainstalowanego systemu operacyjnego, zadanie musi być uruchamiane z poziomu zarządzania serwerem.
Diagnostyka	Wymagany panel LCD umieszczony na froncie obudowy, umożliwiający wyświetlenie informacji o stanie komponentów serwera, w tym co najmniej: procesora, pamięci, dysków, BIOS'u, informacji o zasilaniu oraz temperaturze.
Karta Zarządzania	Niezależna od zainstalowanego na serwerze systemu operacyjnego posiadająca dedykowany port Gigabit Ethernet RJ-45 i umożliwiająca: ▪ zdalny dostęp do graficznego interfejsu Web karty zarządzającej; ▪ zdalne monitorowanie i informowanie o statusie serwera (m.in. prędkości obrotowej wentylatorów, konfiguracji serwera); ▪ szyfrowane połączenie (TLS) oraz autentykację i autoryzację użytkownika; ▪ możliwość podmontowania zdalnych wirtualnych napędów; ▪ wirtualną konsolę z dostępem do myszy, klawiatury; ▪ wsparcie dla IPv6; ▪ wsparcie dla WSMAN (Web Service for Management); SNMP; IPMI2.0, SSH, Redfish; ▪ możliwość zdalnego monitorowania w czasie rzeczywistym poboru prądu przez serwer; ▪ możliwość zdalnego ustawienia limitu poboru prądu przez konkretny serwer; ▪ integrację z usługą katalogową Active Directory; ▪ obsługę przez dwóch administratorów jednocześnie; ▪ wsparcie dla dynamic DNS; ▪ wysyłanie do administratora maila z powiadomieniem o awarii lub zmianie konfiguracji sprzętowej; ▪ możliwość bezpośredniego zarządzania poprzez dedykowany port USB na przednim panelu serwera; ▪ możliwość zarządzania do 100 serwerów bezpośrednio z konsoli karty zarządzającej pojedynczego serwera.
Certyfikaty i normy	▪ Spełnianie postanowień normy ISO 9001 lub równoważnej w zakresie produkcji dla producenta sprzętu - dokumentem potwierdzającym spełnienie wymagań będzie załączony do oferty certyfikat producenta. ▪ Spełnienie postanowień normy ISO 14001 lub równoważnej w zakresie produkcji dla producenta sprzętu - dokumentem potwierdzającym spełnienie wymagań będzie załączony do oferty certyfikat producenta. ▪ Spełnienie postanowień normy ISO 50001 lub równoważnej dla produkcji serwerów przez producenta sprzętu - dokumentem

	potwierdzającym spełnienie wymagań będzie załączony do oferty certyfikat producenta. ▪ Oferowany sprzęt musi posiadać certyfikację oraz oznaczenie CE. ▪ Oferowany sprzęt musi zawierać informacje dotyczące ponownego użycia i recyklingu, nie mogą zawierać farb i powłok na dużych plastikowych częściach, których nie da się poddać recyklingowi lub ponownie użyć. Wszystkie produkty zawierające podzespoły elektroniczne oraz niebezpieczne składniki powinny być bezpiecznie i łatwo identyfikowalne oraz usuwalne. Usunięcie materiałów i komponentów powinno odbywać się zgodnie z wymogami Dyrektywy WEEE 2002/96/EC. Produkty muszą składać się z co najmniej w 65% ze składników wielokrotnego użytku/zdatnych do recyklingu. We wszystkich produktach części tworzyw sztucznych większe niż 25-gramowe powinny zawierać nie więcej niż śladowe ilości środków zmniejszających palność sklasyfikowanych w dyrektywie RE 67/548/EEC. Potwierdzeniem spełnienia powyższego wymogu będzie wydruk ze strony internetowej www.epeat.net potwierdzający spełnienie normy co najmniej Epeat Bronze według normy wprowadzonej w 2019 roku - Wykonawca złoży wraz z ofertą dokument potwierdzający spełnianie wymogu. ▪ Oferowany model serwera musi znajdować się na liście Windows Server Catalog i posiadać status „Certified for Windows” dla systemów Microsoft Windows Server 2016, Microsoft Windows Server 2019, Microsoft Windows Server 2022.
Warunki gwarancyjno-serwisowe	Dla zaoferowanego serwera Zamawiający wymaga następujących warunków gwarancji i serwisu: 1. Minimalny czas trwania gwarancji udzielonej przez producenta na serwer wynosi 24 miesiące. 2. W przypadku awarii dysku twardego (w urządzeniu objętym aktywnym wparciem technicznym) powodującej konieczność jego wymiany, uszkodzony dysk pozostaje u Zamawiającego. 3. Okres zabezpieczenia serwisowego na dyski twarde, o którym mowa w pkt 2 musi odpowiadać okresowi udzielonej gwarancji na sprzęt. 4. Wymagany czas reakcji serwisu na zgłoszenie - do końca następnego dnia roboczego. Wymagana możliwość zgłaszania awarii w trybie 24x7x365 poprzez ogólnopolską linię telefoniczną producenta. 5. Wymagana możliwość sprawdzenia statusu gwarancji poprzez stronę producenta podając unikatowy numer urządzenia oraz pobieranie uaktualnień mikrokodu oraz sterowników nawet w przypadku wygaśnięcia gwarancji serwera

	6. Zaoferowane urządzenie musi mieć możliwość rozszerzenia gwarancji przez producenta do 7 lat.
Dodatkowy okres gwarancji (wymaganie fakultatywne)	Zaoferowanie serwera z dodatkową gwarancją producenta wydłużającą gwarancję podstawową o okres dodatkowych 12, 24, 36 lub więcej miesięcy jest wymogiem nieobowiązkowym (fakultatywnym) i jest kryterium dodatkowo punktowanym zgodnie z kryterium oceny ofert dla Kryterium „gwarancja serwera (KG2)" **Potwierdzenie spełnienia tego kryterium Wykonawca zaznacza w formularzu ofertowym.**
Dokumentacja użytkownika	Zamawiający wymaga dokumentacji w języku polskim lub angielskim. Musi istnieć możliwość telefonicznego sprawdzenia konfiguracji sprzętowej serwera oraz warunków gwarancji po podaniu numeru seryjnego bezpośrednio u producenta lub jego przedstawiciela.

6. MACIERZ

ATRYBUT	MINIMALNE WYMAGANIA FUNKCJONALNE, TECHNICZNE, UŻYTKOWE, JAKOŚCIOWE
Ilość	1 zestaw
Określenie oferowanej konfiguracji	Zamawiający wymaga określenia przez oferenta w formularzu ofertowym co najmniej następujących cech oferowanego rozwiązania: producent (marka), model (symbol), rodzaj obudowy, rodzaj i ilość dysków twardych, gwarancja
Funkcjonalność obudowy	1. Do instalacji w standardowej szafie Rack 19", z kompletem szyn teleskopowych, macierz musi zajmować maksymalnie wysokość 2U, wyposażona w 8 zatok na dyski twarde 2.5"/3.5" SATA3 z możliwością konfiguracji Hot Swap. 2. Na potrzeby przyszłej rozbudowy musi istnieć możliwość rozszerzenia (rozbudowy) na 16 zatok za pomocą dedykowanego rozwiązania. 3. Wyposażona w wskaźniki LED informujące co najmniej o statusach: HDD 1-8, Status, LAN. 4. Wyposażona w porty: 4x USB 3.2 Gen1.
Pamięć	1. Min. 4GB RAM z możliwością rozszerzenia do 16GB 2. Min. 512MB Flash 3. 4 szt. HDD SATA3 o pojemności min. 4TB każdy, wyposażone w bufor min. 256MB, przystosowanych do zapisu ciągłego, kompatybilnych z oferowanym urządzeniem
Obsługiwane systemy plików	1. Dyski wewnętrzne EXT4. 2. Dyski zewnętrzne EXT3, EXT4, NTFS, FAT32, HFS+, exFAT

Zarządzanie dyskami	SMART, sprawdzanie bad sektorów
Obsługa (funkcje) RAID	1. Pojedynczy dysk, JBOD, RAID 0, 1, 5, 5+Spare, 6, 6+Spare, 10, 10+Spare, 50/60. 2. Możliwość zwiększania pojemności i migracja między poziomami RAID online. 3. Przywracanie RAID.
Szyfrowanie	1. Możliwość szyfrowania całych woluminów oraz folderów współdzielonych kluczem AES 256 bitów. 2. Mechanizm szyfrowania z akceleracją sprzętową.
Interfejsy sieciowe	2x 2,5GbE (2.5G/1G/100M/10M) 1x 10GbE SFP+
Protokoły	Wymagana obsługa co najmniej następujących protokołów: CIFS, AFP, NFS, FTP, WebDAV, iSCSI, Telnet, SSH, SNMP
Usługi	Wsparcie dla: Windows ACL, Serwer wydruku, Serwer WWW, Serwer plików, Manager plików przez WWW, Obsługa paczek QPKG, Funkcja Virtual Disk umożliwiająca zwiększenie pojemności serwera przy pomocy protokołu iSCSI, Replikacja w czasie rzeczywistym, Klient LDAP, Serwer Syslog, Migawki wolumenów, Obsługa kontenerów (LXC – Docker), Serwer VPN
Język GUI	Polski
iSCSI	Obsługa MPIO, MC/S i SPC-3 Persistent Reservation
Liczba kont użytkowników	4096
Liczba grup	512
Liczba udziałów	512
Max ilość połączeń	700
Zasilanie	Redundatne PSU 2x250W
Wentylatory	Minimum 2
Współpraca z UPS	Wymagana obsługa sieciowych awaryjnych zasilaczy UPS.
Certyfikaty i normy	Oferowany sprzęt musi posiadać certyfikację oraz oznaczenie CE
Warunki gwarancyjno-serwisowe	Gwarancja producenta min. 2 lata (24 miesiące) na urządzenie + dyski
Dodatkowy okres gwarancji (wymaganie fakultatywne)	Zaoferowanie macierzy z dodatkową gwarancją producenta wydłużającą gwarancję podstawową o okres dodatkowych 12 miesięcy jest wymogiem nieobowiązkowym (fakultatywnym) i jest kryterium dodatkowo punktowanym zgodnie z kryterium oceny ofert dla Kryterium „gwarancja macierzy (KG3)” **Potwierdzenie spełnienia tego kryterium Wykonawca zaznacza w formularzu ofertowym.**

7. SERWER BACKUPOWY - TYP 1

ATRYBUT	MINIMALNE WYMAGANIA FUNKCJONALNE, TECHNICZNE, UŻYTKOWE, JAKOŚCIOWE
Ilość	1 zestaw
Określenie oferowanej konfiguracji	Zamawiający wymaga określenia przez oferenta w formularzu ofertowym co najmniej następujących cech oferowanego rozwiązania: producent (marka), model (symbol), procesor, rodzaj obudowy, rodzaj i ilość dysków twardych, gwarancja
Procesor	Wymagany procesor klasy x86 wielordzeniowy, umożliwiający osiągnięcie w teście Passmark CPU Mark, w kategorii Average CPU Mark wynik min. 17000 punktów. **Dokumentem potwierdzającym spełnienie wymagań będzie złożony przez Wykonawcę wydruk ze strony www.cpubenchmark.net**
Funkcjonalność obudowy	1. Do instalacji w standardowej szafie Rack 19", z kompletem szyn teleskopowych, serwer musi zajmować maksymalnie wysokość 2U 2. Wyposażona w wskaźniki LED informujące co najmniej o statusach: HDD 1-8, Status, LAN.
Porty i gniazda	Wymagane co najmniej: 4x PCIe Gen 3 (x4) 4x USB 3.2 Gen1, 1x gniazdo typu C USB 3.2 Gen2 5V/3A 10 Gb/s, 1x gniazdo typu A USB 3.2 Gen2 5V/1A 10 Gb/s
Pamięć	1. Min. 8GB RAM z możliwością rozszerzenia do 64GB 2. Min. 5GB Flash (DOM) 3. 6 szt. HDD SATA3 o pojemności min. 4TB każdy, wyposażone w bufor min. 256MB, przystosowanych do zapisu ciągłego, kompatybilnych z oferowanym urządzeniem
Obsługiwane systemy plików	1. Dyski wewnętrzne EXT4. 2. Dyski zewnętrzne EXT3, EXT4, NTFS, FAT32, HFS+
Zarządzanie dyskami	SMART, sprawdzanie bad sektorów
Obsługa (funkcje) RAID	1. Pojedynczy dysk, JBOD, RAID 0,1,5 ,6 ,10, 50, 60. 2. Możliwość zwiększania pojemności i migracja między poziomami RAID online. 3. Obsługa BITMAP w celu przyspieszenia odbudowy. 4. Możliwość skonfigurowania Global Spare Disk.
Szyfrowanie	Możliwość szyfrowania całych woluminów oraz folderów współdzielonych kluczem AES 256 bitów.

Interfejsy sieciowe	2x Gigabit (10/100/1000) RJ-45 2x 10GbE SFP+ Wymagana obsługa VLAN i Jumbo Frame.
Protokoły	Wymagana obsługa co najmniej następujących protokołów: CIFS, AFP, NFS, FTP, WebDAV, iSCSI, Telnet, SSH, SNMP
Usługi	Wsparcie dla: Windows ACL, Integracja w Windows ADS, Serwer wydruku, Serwer WWW, Serwer plików, Manager plików przez WWW, Obsługa paczek QPKG, Funkcja Virtual Disk umożliwiająca zwiększenie pojemności serwera przy pomocy protokołu iSCSI, Montowanie obrazów ISO, Replikacja w czasie rzeczywistym, Serwer RADIUS, Klient LDAP, Serwer Syslog, Serwer TFTP, Server VPN, Obsługa kontenerów (LXC, Docker), Autotiering, Migawki wolumenów
Wirtualizacja	Wymagana możliwość uruchomienia maszyn wirtualnych bezpośrednio na urządzeniu bez konieczność posiadania zewnętrznych wirtualizatorów
SSD Cache	Wsparcie dla pamięci podręcznej (SSD cache) w trybach: tylko odczyt, odczyt-zapis, tylko zapis
Język GUI	Polski
iSCSI	Obsługa MPIO, MC/S i SPC-3 Persistent Reservation
Liczba kont użytkowników	4096
Liczba grup	512
Liczba udziałów	512
Max ilość połączeń	700
Zasilanie	Redundantne PSU 2x 300W
Wentylatory	Minimum 2
Współpraca z UPS	Wymagana obsługa sieciowych awaryjnych zasilaczy UPS.
Certyfikaty i normy	Oferowany sprzęt musi posiadać certyfikację oraz oznaczenie CE
Warunki gwarancyjno-serwisowe	Gwarancja producenta min. 2 lata (24 miesiące) na urządzenie + dyski
Dodatkowy okres gwarancji (wymaganie fakultatywne)	Zaoferowanie serwera backupu z dodatkową gwarancją producenta wydłużającą gwarancję podstawową o okres dodatkowych 12 miesięcy jest wymogiem nieobowiązkowym (fakultatywnym) i jest kryterium dodatkowo punktowanym zgodnie z kryterium oceny ofert dla Kryterium „gwarancja serwera backupu - typ 1 (KG4)” **Potwierdzenie spełnienia tego kryterium Wykonawca zaznacza w formularzu ofertowym.**

8. SERWER BACKUPOWY - TYP 2

ATRYBUT	MINIMALNE WYMAGANIA

	FUNKCJONALNE, TECHNICZNE, UŻYTKOWE, JAKOŚCIOWE
Ilość	1 zestaw
Określenie oferowanej konfiguracji	Zamawiający wymaga określenia przez oferenta w formularzu ofertowym co najmniej następujących cech oferowanego rozwiązania: producent (marka), model (symbol), rodzaj obudowy, rodzaj i ilość dysków twardych, gwarancja
Funkcjonalność obudowy	1. Do instalacji w standardowej szafie Rack 19", z kompletem szyn teleskopowych, serwer musi zajmować maksymalnie wysokość 1U, wyposażona w 4 zatoki na dyski twarde 2.5"/3.5" SATA3 z możliwością konfiguracji Hot Swap. 2. Wyposażona w wskaźniki LED informujące co najmniej o statusach: HDD 1-4, Status, LAN. 3. Wyposażona w porty: 4x USB 3.2 Gen1.
Pamięć	1. Min. 2GB RAM z możliwością rozszerzenia do 8GB 2. Min. 512MB Flash 3. 2 szt. HDD SATA3 o pojemności min. 4TB każdy, wyposażone w bufor min. 256MB, przystosowanych do zapisu ciągłego, kompatybilnych z oferowanym urządzeniem
Obsługiwane systemy plików	1. Dyski wewnętrzne EXT4. 2. Dyski zewnętrzne EXT3, EXT4, NTFS, FAT32, HFS+
Zarządzanie dyskami	SMART, sprawdzanie bad sektorów
Obsługa (funkcje) RAID	1. Pojedynczy dysk, JBOD, RAID 0,1,5 ,6 ,10. 2. Możliwość zwiększania pojemności i migracja między poziomami RAID online 3. Obsługa BITMAP w celu przyspieszenia odbudowy. 4. Możliwość skonfigurowania Global Spare Disk.
Szyfrowanie	1. Możliwość szyfrowania całych woluminów oraz folderów współdzielonych kluczem AES 256 bitów. 2. Mechanizm szyfrowania z akceleracją sprzętową.
Interfejsy sieciowe	2x Gigabit (10/100/1000) RJ-45 1x 10GbE SFP+ Wymagana możliwość podłączenia dongle wireless przez port USB, obsługa VLAN i Jumbo Frame.
Protokoły	Wymagana obsługa co najmniej następujących protokołów: CIFS, AFP, NFS, FTP, WebDAV, iSCSI, Telnet, SSH, SNMP
Usługi	Wsparcie dla: Windows ACL, Integracja w Windows ADS, Serwer wydruku, Serwer WWW, Serwer plików, Manager plików przez WWW, Obsługa paczek QPKG, Funkcja Virtual Disk umożliwiająca zwiększenie pojemności serwera przy pomocy protokołu iSCSI, Montowanie obrazów ISO, Replikacja w czasie rzeczywistym, Serwer RADIUS, Klient LDAP,

	Serwer Syslog, Migawki wolumenów, Obsługa kontenerów (LXC – Docker)
Język GUI	Polski
iSCSI	Obsługa MPIO, MC/S i SPC-3 Persistent Reservation
Liczba kont użytkowników	4096
Liczba grup	512
Liczba udziałów	512
Max ilość połączeń	700
Zasilanie	Zasilacz o moc min. 100W
Wentylatory	Minimum 2
Współpraca z UPS	Wymagana obsługa sieciowych awaryjnych zasilaczy UPS.
Certyfikaty i normy	Oferowany sprzęt musi posiadać certyfikację oraz oznaczenie CE
Warunki gwarancyjno-serwisowe	Gwarancja producenta min. 2 lata (24 miesiące) na urządzenie + dyski

9. PRZEŁĄCZNIKI SIECIOWE ZARZĄDZALNE

ATRYBUT	MINIMALNE WYMAGANIA FUNKCJONALNE, TECHNICZNE, UŻYTKOWE, JAKOŚCIOWE
Ilość	2 zestawy
Określenie oferowanej konfiguracji	Zamawiający wymaga określenia przez oferenta w formularzu ofertowym co najmniej następujących cech oferowanego rozwiązania: producent (marka), model (symbol), gwarancja.
Obudowa	Do montażu w szafie Rack 19”, o wysokości nie więcej niż 1U, wraz z kompletem odpowiednich szyn, wyposażona w wewnętrzny zasilacz 230V AC.
Porty	1. 48 portów 100M/1000M Base-T RJ45. 2. 4 porty 1G/10G SFP+. 3. Port USB umożliwiający podłączenie zewnętrznej pamięci flash.
Wymagane mechanizmy związane z zapewnieniem bezpieczeństwa sieci	1. Nie mniej niż 4 poziomy dostępu administracyjnego poprzez konsolę. 2. Wymagana autoryzacja użytkowników w oparciu o IEEE 802.1x z możliwością przydziału VLANu oraz dynamicznego przypisania listy ACL. 3. Możliwość utworzenia minimum 2000 list ACL. 4. Możliwość uwierzytelniania urządzeń na porcie w oparciu o adres MAC oraz poprzez portal www. 5. Zarządzanie urządzeniem przez HTTPS, SNMP i SSHv2 za pomocą protokołów IPv4 i IPv6.

	6. Możliwość filtrowania ruchu w oparciu o adresy MAC, IPv4, IPv6, porty TCP/UDP. 7. Obsługa mechanizmów Port Security, Dynamic ARP Inspection, IP Source Guard, voice VLAN oraz private VLAN (lub równoważny) - możliwość synchronizacji czasu zgodnie z NTP. 8. Obsługa funkcjonalności DLDP lub równoważnej.
Wymagane opcje zarządzania	1. Możliwość lokalnej i zdalnej obserwacji ruchu na określonym porcie, polegająca na kopiowaniu pojawiających się na nim ramek i przesyłaniu ich do urządzenia monitorującego przyłączonego do innego portu oraz poprzez określony VLAN. 2. Plik konfiguracyjny urządzenia musi być możliwy do edycji w trybie off-line (tzn. konieczna jest możliwość przeglądania i zmian konfiguracji w pliku tekstowym na dowolnym urządzeniu PC). 3. Urządzenie musi posiadać wbudowany port USB, pozwalający na podłączenie zewnętrznej pamięci FLASH w celu przechowywania obrazów systemu operacyjnego, plików konfiguracyjnych lub certyfikatów elektronicznych. 4. Dedykowany port konsoli musi być zgodny ze standardem RS-232. 5. Dedykowany port zarządzający out-of-band Ethernet 10/100Base-T.
Łączenie w stos	Przełącznik musi umożliwiać łączenie w stosy z zachowaniem następującej funkcjonalności: 1. Zarządzanie stosem poprzez jeden adres IP. 2. Do min. 9 jednostek w stosie. 3. Możliwość tworzenia połączeń link aggregation zgodnie z 802.3ad dla portów należących do różnych jednostek w stosie (ang. cross-stack link aggregation). 4. Stos przełączników powinien być widoczny w sieci jako jedno urządzenie logiczne z punktu widzenia protokołu Spanning-Tree
Wydajność urządzenia	1. Układ przełączający o wydajności min. 176 Gbps, wydajność przełączania przynajmniej 132 Mpps 2. Obsługa min. 32 000 adresów MAC 3. Wbudowana pamięć RAM min. 512 MB 4. Urządzenie musi mieć wbudowaną pamięć flash o pojemności min. 512 MB 5. Obsługa min. 4000 sieci VLAN jednocześnie oraz obsługa 802.1Q tunneling (QinQ) 6. Możliwość skonfigurowania min. 1024 interfejsów vlan interface SVI działających równocześnie 7. Obsługa ramek jumbo o wielkości min. 9216 bajtów 8. Obsługa protokołu GVRP lub równoważnego

	9. Wsparcie dla protokołów IEEE 802.1w Rapid Spanning Tree oraz IEEE 802.1s Multi-Instance Spanning Tree. Wymagane wsparcie dla min. 64 instancji protokołu MSTP 10. Obsługa min. 4096 tras dla routingu IPv4 11. Obsługa min. 1024 tras dla routingu IPv6 12. Obsługa protokołów routingu OSPF, OSPFv3, RIPv1, RIPv2, RIPng, PIM-SM, PIM-DM. Jeżeli do obsługi powyższych funkcjonalności wymagana jest licencja to należy ją dostarczyć w ramach niniejszego postępowania 13. Obsługa wirtualnych tablic routingu-forwardingu (VRF) 14. Obsługa protokołów LLDP i LLDP-MED 15. Przełącznik musi posiadać funkcjonalność DHCP Server 16. Obsługa ruchu multicast: IGMP v1, v2 i v3, IGMP Snooping v1, v2 i v3; MLD Snooping.
Obsługa ruchu sieciowego	Wymagana implementacja co najmniej ośmiu kolejek sprzętowych QoS na każdym porcie wyjściowym z możliwością konfiguracji dla obsługi ruchu o różnych klasach: 1. Klasyfikacja ruchu do klas różnej jakości obsługi (QoS) poprzez wykorzystanie następujących parametrów: źródłowy adres MAC, docelowy adres MAC, źródłowy adres IP, docelowy adres IP, źródłowy port TCP, docelowy port TCP. 2. Wsparcie dla minimum dwóch różnych mechanizmów QoS z wykorzystaniem algorytmu karuzelowego. 3. Urządzenie musi posiadać mechanizm do badania jakości połączeń (IP SLA) z możliwością badania takich parametrów jak: jitter, opóźnienie, straty pakietów dla wygenerowanego strumienia testowego UDP. Urządzenie musi mieć możliwość pracy jako generator oraz jako odbiornik pakietów testowych IP SLA. Urządzenie musi umożliwiać konfigurację liczby wysyłanych pakietów UDP w ramach pojedynczej próbki oraz odstępu czasowego pomiędzy kolejnymi wysyłanymi pakietami UDP w ramach pojedynczej próbki. Jeżeli funkcjonalność IP SLA wymaga licencji to Zamawiający wymaga jej dostarczenia w ramach niniejszego postępowania.
Pozostałe wymagania	1. System operacyjny (firmware) musi być dostarczony przez producenta urządzenia. Zamawiający nie dopuszcza dostarczenia urządzenia z zainstalowanym systemem operacyjnym firmy trzeciej. 2. Wymagana pełna dokumentacja w języku polskim lub angielskim.
Certyfikaty i normy	Oferowany sprzęt musi posiadać certyfikację oraz oznaczenie CE
Warunki gwarancyjno-serwisowe	1. Minimalny czas trwania gwarancji udzielonej przez producenta na urządzenie wynosi 36 miesięcy. Wymagane dostarczenie części zamiennych w trybie 9x5xNBD.

	2. Wymagany bezpłatny dostęp do najnowszych wersji oprogramowania na stronie producenta przez cały okres gwarancji urządzenia.

10. MODERNIZACJA SIECI STRUKTURALNEJ LAN

MINIMALNE WYMAGANIA FUNKCJONALNE, TECHNICZNE, UŻYTKOWE, JAKOŚCIOWE
Informacje ogólne Zadaniem Wykonawcy jest realizacja prac instalacyjnych obejmujących rozbudowę sieci strukturalnej LAN (sieci komputerowej) w budynku Urzędu Gminy, przez dostawę kompletnego systemu okablowania strukturalnego. Wykonawca jest zobowiązany do wykonania instalacji okablowania zgodnie z wymaganiami Zamawiającego opisanymi w niniejszym dokumencie oraz zgodnie z wymaganiami norm obowiązujących w tym zakresie.
Stan bieżący, stan oczekiwany Aktualny stan przedstawia 30 pojedynczych punktów abonenckich LAN w kategorii kat.6. Wymagana jest rozbudowa istniejącej sieci LAN w kategorii 6 do 47 podwójnych gniazd LAN (94 linie) oraz zainstalowanie jednego punktu dostępowego w Sali narad i podłączenie go do sieci linią kablową. Ilość i lokalizację gniazd oraz punktów dystrybucyjnych przyjęto na podstawie aktualnych potrzeb i wytycznych Zamawiającego. W przypadku zmiany koncepcji rozmieszczenia gniazd, ostateczna i precyzyjna lokalizacja gniazd logicznych powinna być ustalona między Zamawiającym, a Wykonawcą w trakcie realizacji. Rozbudowa sieci strukturalnej zakłada również sprawdzenie poprawności działania istniejącej sieci oraz naprawę istniejących nieprawidłowości. Zamawiający dopuszcza wykorzystanie istniejących punktów abonenckich. W przypadku braku możliwości dołożenia drugiego modułu do istniejącego punktu abonenckiego wymagana jest wymiana punktu abonenckiego na nowy.
Podstawą do zaprojektowania systemu powinna być wizja lokalna przeprowadzona przez Wykonawcę. 1. Zamawiający zaleca Wykonawcom przeprowadzenie wizji lokalnej celem uzyskania wszystkich niezbędnych informacji do prawidłowego oszacowania kosztów oraz zakresu prac. Każdy z Wykonawców ponosi pełną odpowiedzialność za skutki braku rozpoznania warunków technicznych do realizacji zadania bądź błędnego rozpoznania tych warunków. 2. Podczas wizji lokalnej, Zamawiający wskaże pomieszczenia, do których należy doprowadzić sieć strukturalną oraz wskaże miejsca, w których należy zakończyć ją punktem logicznym. Zamawiający informuje, że nie posiada ani profesjonalnych projektów, ani przedmiarów dotyczących budowy sieci teleinformatycznej. Podstawą do opracowania zagadnień związanych z okablowaniem strukturalnym muszą być normy okablowania strukturalnego. <u>Normy europejskie dotyczące okablowania strukturalnego - wymagań ogólnych i specyficznych dla danego środowiska:</u>

ISO/IEC 11801-1:2017- Information technology - Generic cabling for customer premises
PN-EN 50173-2:2018-07 - wersja angielska - Technika Informatyczna – Systemy okablowania strukturalnego
Część 1: Wymagania ogólne,
Część 2: Budynki biurowe.

Normy europejskie pomocnicze - w zakresie instalacji:
PN-EN 50174-1:2018-08 - wersja angielska - Technika informatyczna - Instalacja okablowania
Część 1 - Specyfikacja instalacji i zapewnienie jakości,
Część 2 - Planowanie i wykonawstwo instalacji wewnątrz budynków,

PN-EN 50346:2004/A2:2010 - wersja polska - Technika informatyczna - Instalacja okablowania - Badanie zainstalowanego okablowania
PN-EN 50310:2016-09 - Sieci połączeń wyrównawczych w budynkach i innych obiektach budowlanych z instalacjami telekomunikacyjnymi

W przypadku powołań normatywnych niedatowanych obowiązuje zawsze najnowsze wydanie cytowanej normy.
Wykonawca ma obowiązek wykonać instalację okablowania zgodnie z wymaganiami norm obowiązujących w czasie realizacji zadania, przy uwzględnieniu wszystkich wymagań opisanych w dokumentach wskazanych powyżej.

Wykonany system okablowania oraz wydajność komponentów na etapie oddania instalacji do użytku musi pozostać w zgodzie z wymaganiami norm PN-EN50173-1:2011 i ISO/IEC11801:2011.

Wytyczne i zalecenie instalacyjne dla zaprojektowania instalacji okablowania strukturalnego w systemie „zaprojektuj i wybuduj"

1. Instalacja musi zostać wykonana w sposób profesjonalny używając do tego celu najlepszych urządzeń i narzędzi oraz korzystając z instalatorskiego doświadczenia Wykonawcy.
2. Określając nowe trasy dla kabli logicznych należy uwzględnić konstrukcję budynku oraz bezkolizyjność z innymi instalacjami i urządzeniami oraz zaplanować ją w taki sposób, aby wszystkie trasy przebiegały wzdłuż linii prostych równoległych i prostopadłych do ścian i stropów zmieniając swój kierunek tylko w zależności od potrzeb (tynki, rozgałęzienia, podejścia do urządzeń). Zamawiający zaleca wykorzystanie istniejących tras kablowych.
3. Przy realizacji tras kablowych pod potrzeby okablowania należy wziąć pod uwagę wymagania normy PN-EN 50174-2:2010/A1:2011 dotyczące równoległego prowadzenia różnych instalacji w budynku, m.in. instalacji zasilającej i zapewnić odpowiednie odległości pomiędzy okablowaniem.
4. Trasy kablowe - pionowe należy wykonać z trwałych elementów umożliwiających przymocowanie kabli oraz zachowanie odpowiednich promieni gięcia kabli na zakrętach. Rozmiary (pojemność) kanałów kablowych należy dobrać uwzględniając maksymalną liczbę

kabli zaprojektowanych w danym miejscu instalacji przy uwzględnieniu co najmniej 20% wolnej przestrzeni na potrzeby ewentualnej rozbudowy systemu.

5. W przypadku mocowania instalacji do konstrukcji wsporczych należy przestrzegać utrzymania jednakowych wysokości zamocowania wsporników i odległości między punktami podparcia.
6. Maksymalna długość kabla instalacyjnego skrętkowego (od punktu dystrybucyjnego do gniazda końcowego) nie może w żadnym przypadku przekroczyć 90 metrów.
7. Wszystkie cztery pary każdego kabla powinny być zakończone w pojedynczym module.
8. Wymaga się standardowej sekwencji połączeń T568A lub T568B.
9. Okablowanie powinno być ciągłe na całej długości toru bez złącz i spawów od stanowiska roboczego do panelu rozdzielczego.
10. Każdy kabel powinien mieć trwałe oznaczenie na dwóch końcach przy zakończonych modułach wg. przyjętego systemu numeracji.
11. Proces montażu ma gwarantować najwyższą powtarzalność. Maksymalny rozplot pary transmisyjnej na złączu modularnym RJ45 nie może być większy niż 6 mm.
12. Okablowanie powinno być prowadzone w sposób uporządkowany i zgodnie z wytycznymi producenta. Wszystkie używane opaski kablowe powinny być ręcznie zaciskane tylko w punktach gdzie nie ma zagięć i skręceń. Kabel nie może być narażony na nacisk i naprężenia wzdłuż drogi prowadzenia kabla i na jego końcach.

Założenia dla systemu okablowania strukturalnego:

1. W celu zapewnienia poprawności obsługi wszystkich aplikacji transmisji danych oraz uzyskania marginesów pracy (maksymalnych zapasów transmisyjnych), system okablowania strukturalnego wraz z jego komponentami oraz kablami przyłączeniowymi musi być wykonany przez producenta jako kompletne rozwiązanie o takich samych parametrach wydajnościowych dla wszystkich elementów okablowania strukturalnego.
2. Zaprojektowane rozwiązanie musi pochodzić od jednego dostawcy systemu okablowania strukturalnego. Niedopuszczalne jest stosowanie rozwiązań składanych od różnych producentów i różnych dostawców komponentów rozumiane jako różne źródła dostaw: kabli, gniazd RJ45, paneli krosowych, kabli krosowych itd.
3. Wszystkie komponenty użyte do budowy pasywnej infrastruktury kablowej muszą być zgodne z wymaganiami obowiązujących norm wg.: ISO/IEC 11801, EN 50173-1, ANSI/TIA/EIA 568-C.2.

Wymagania dla kabla instalacyjnego

W obiekcie projektuje się instalację teletechniczną, która wykonana będzie jako nie/ekranowana sieć okablowania strukturalnego klasy E (komponenty minimum kategorii 6), poprowadzona kablem o paśmie przenoszenia minimum 450 MHz. Kabel musi spełniać wymagania poniższych norm:

- EN 50173-1:2018-07
- ISO/IEC 11801 Edition 2.2
- ANSI/TIA-568-C.0; C.1; C.2
- IEC 60754-2

Do każdego portu RJ45 punktu logicznego należy doprowadzić kabel skrętkowy 4-parowy. Każdy kabel skrętkowy, 4-parowy należy zakończyć na pojedynczym module RJ45 (gnieździe RJ45). Nie dopuszcza się rozdziału jednego kabla 4-parowego na większą ilość portów (nie dopuszcza się wkładek i przejściówek rozdzielających). Kabel ten ma zapewniać pozytywne parametry transmisyjne w całym paśmie minimum 450MHz. Projektowany kabel musi posiadać zewnętrzną powłokę LSOH nie wydzielającą szkodliwych toksyn podczas spalania. Wymaga się, aby kabel posiadał euroklasę min. Dca zgodnie z dyrektywą CPR.

Minimalne wymagania dla kabla:

Częstotliwość pracy	Do 450MHz
Rodzaj ekranowania	U/UTP (kabel nieekranowany)
Powłoka zewnętrzna	LSOH (Low Smoke Zero Halogen)
Średnica przewodnika	24AWG
Średnica zewnętrzna	5,3mm ± 0.2mm
Euroklasa	Dca- s2,d2,a1
Zakres temperatur	Instalacja: -10°C do +50°C Praca: -30°C do +70°C
NVP	69% (0.69)

W celu potwierdzenia wymaganych parametrów oraz zgodności z normami EN50173, ISO11801, TIA-568.2-D producent oferowanego kabla musi posiadać certyfikat wydany przez niezależne laboratorium (np. DELTA, Intertek, GHMT).

Punkt logiczny sieci

W celu łatwego zarządzania okablowaniem strukturalnym każdy moduł RJ45 w punkcie logicznym musi posiadać oznaczanie jednoznacznie je identyfikujące. Numeracja gniazd logicznych sieci komputerowej powinna zostać uzgodniona z przedstawicielem Zamawiającego.

Punkty logiczne PL (gniazda przyłączeniowe użytkowników) należy zorganizować w postaci modułów RJ45 keystone montowanych w adapterze z tworzywa sztucznego o wymiarach 45x45mm (format Mosaic).

Punkty logiczne należy wykonać w oparciu o nieekranowane moduły typu keystone kategorii 6 mocowane w odpowiednich adapterach dopasowanych do osprzętu elektroinstalacyjnego.

Moduł musi spełniać wymagania kategorii 6 (klasy E) wg poniższych norm:

- EN 50173-1:2018-07
- EN 50173-1:2011
- ISO/IEC 11801 Edition 2.2
- ANSI/TIA-568-C.0
- ANSI/TIA-568-C.1
- ANSI/TIA-568-C.2
- IEC 60603-7

Wymagania minimalne dla modułu RJ45

Średnica przewodnika	Od 26 do 23AWG
Obsługa PoE	PoE, PoE+, 4PPoE, Power over HDBase-T
Częstotliwość	250MHz
Rodzaj	Beznarzędziowy
Zabezpieczenie	Automatyczna klapka przeciwkurzowa
Trwałość	1000-krotność wpięć/wypięć

Zgodność modułu RJ45 z powyższymi normami musi zostać potwierdzona certyfikatem niezależnego laboratorium badawczego (np. DELTA Force Technology).

Moduł RJ45 kat. 6 musi posiadać zintegrowaną, automatyczną klapkę przeciwkurzową, dzięki czemu zapewniona będzie szczelność, gdy gniazdo jest nieużywane. Klapka ma za zadanie chronić piny przed zakurzeniem oraz ochronić przed wytworzenia łuków elektrycznych przy wpinaniu gdy zasilanie jest prowadzone przez skrętkę (PoE).

Podczas realizacji przedsięwzięcia należy użyć modułów zarabianych beznarzędziowo. Maksymalny rozplot pary transmisyjnej nie może być większy niż 6mm od złącza.

Moduł musi być zgodny ze standardem Keystone. Złącza IDC modułów powinny mieć możliwość podłączenia żył o AWG 23-26. Moduł powinien posiadać oznaczenia kolorystyczne ułatwiające przyłączenie kabla w sekwencji 568B lub 568A.

Panel krosowniczy

Zakończenie kabli projektuje się w szafie teleinformatycznej Rack na panelach modularnych. Panele rozdzielcze powinny umożliwiać wpinanie 24 modułów RJ45 typu keystone, takich samych jak w gniazdach abonenckich. Panel powinien posiadać 24 porty i wysokość 1U. Panel musi posiadać zintegrowaną prowadnicę kabli przychodzących, co zapewni swobodne uchwycenie kabli i eliminacje naprężeń związanych z wagą doprowadzonych kabli. Patchpanel musi być wyposażony w gwintowane przyłącze linki uziemienia panela. Wszystkie zainstalowane panele muszą być podłączone poprzez ww. przyłącze do szyny uziemienia szafy.

Punkt dostępowy sieci WiFi

1. Wymagany jest montaż 1 (jednego) urządzenia w Sali narad.
2. Urządzenie musi być wyposażone w min. 2 porty RJ45 pracujące z prędkością 1Gb/s obsługujący standard PoE 802.3af oraz pasywne zasilanie PoE.
3. Urządzenie musi być wyposażone w przycisk przywracania ustawień.
4. Urządzenie musi być wyposażone w min. 3 anteny wewnętrzne dookólne o zysku min 3dBi dla sieci 2,4GHz oraz min 4dBi dla sieci 5GHz.
5. Urządzenie musi pracować w standardzie IEEE 802.11ac/n/g/b/a oraz częstotliwości pracy 2,4 oraz 5GHz.

6. Urządzenie powinno być dostosowane do montażu na ścianie lub suficie oraz posiadać dołączony zestaw montażowy. 7. Urządzenie musi pracować zarówno jako urządzenie typu stand-alone lub w trybie podłączonym do kontrolera sieci bezprzewodowej. 8. Urządzenie musi posiadać funkcjonalność tworzenia wielu sieci WiFi - min. 14 SSID 9. Urządzenie musi posiadać funkcjonalność: wyłącznik sieci bezprzewodowej, automatyczny wybór kanału, kontrola mocy transmisji, QoS (WMM), sterowanie pasmem, równoważenie obciążenia pasma, kontrola przepustowości, harmonogram resetu oraz sieci bezprzewodowej. 10. Urządzenie musi posiadać możliwość utworzenia strony powitalnej. 11. Urządzenie musi posiadać możliwość mapowania SSID do VLAN oraz izolowania klientów sieci bezprzewodowej. 12. Urządzenie musi być zarządzane z poziomu przeglądarki internetowej oraz obsługiwać zarządzanie poprzez HTTPS. 13. Urządzenie musi posiadać obsługę SNMP v1/v2c. 14. W zestawie z urządzeniem powinien być dostarczony adapter zasilania pasywnego PoE, kabel zasilający oraz zestaw montażowy.
Pomiary i badania instalacji okablowania strukturalnego. Przed rozpoczęciem prac istniejącą instalację sieci strukturalnej LAN należy poddać pomiarom i badaniom sprawdzającym. W przypadku wykrycia nieprawidłowości należy je wyeliminować. Po zrealizowaniu prac instalacyjnych polegających na rozbudowie sieci strukturalnej LAN, wykonaną instalację należy poddać pomiarom i badaniom sprawdzającym. W zakres pomiarów wchodzą wszystkie interfejsy okablowania poziomego oraz szkieletowego.
Poziom usług (wymaganie fakultatywne) W celu zapewnienia wysokiego poziomu wykonywanych zadań, podmiot realizujący usługę polegającą na modernizacji sieci LAN powinien posiadać wdrożony system zarządzania jakością potwierdzony aktualnym certyfikatem ISO 9001 w zakresie świadczenia usług w obszarze projektowania i wykonawstwa sieci teleinformatycznych - wymaganie ma charakter nieobowiązkowy (fakultatywny) i jest kryterium dodatkowo punktowanym zgodnie z kryterium oceny ofert dla Kryterium „jakościowym (KJ)” **Potwierdzenie spełnienia tego kryterium Wykonawca zaznacza w formularzu ofertowym.**

11. LICENCJE NA SYSTEM OPERACYJNY ORAZ WIRTUALIZACJĘ, LICENCJE DOSTĘPOWE

MINIMALNE WYMAGANIA FUNKCJONALNE, TECHNICZNE, UŻYTKOWE, JAKOŚCIOWE
1. Licencje bezterminowe (wieczyste) na oprogramowanie muszą zostać dostarczone dla serwera fizycznego o którym mowa w punkcie 5 niniejszego załącznika. Jeśli dobór licencji zależy od liczby rdzeni procesora (procesorów) w serwerze, Wykonawca ma obowiązek dostarczyć właściwą liczbę licencji dla liczby wszystkich rdzeni wszystkich zastosowanych procesorów w oferowanym serwerze.

2. Licencja na serwerowy system operacyjny musi uprawniać do uruchamiania serwerowego systemu operacyjnego w środowisku fizycznym i 4 wirtualnych środowisk serwerowego systemu operacyjnego.
3. Jeśli do legalnego korzystania z oprogramowania serwera (w zgodzie z licencją) jest wymagana licencja dostępowa (Client Access License) zapewniająca użytkownikowi prawo do korzystania z usług serwera, to należy przewidzieć dostawę sumarycznie 50 licencji dostępowych na urządzenie współpracujących z oferowanym systemem operacyjnym.
4. System musi być nowy (nie aktywowany wcześniej na innym urządzeniu).
5. Zamawiający wymaga dostarczenia licencji na oprogramowanie (system serwerowy) w najnowszej wersji obecnie dostępnej na rynku.
6. W ofercie wymagane jest podanie modelu, symbolu oraz producenta oferowanego oprogramowania oraz jego nazwę handlową.

Serwerowy system operacyjny musi posiadać następujące wymagania minimalne:

1. Możliwość wykorzystania 320 logicznych procesorów oraz co najmniej 4 TB pamięci RAM w środowisku fizycznym.
2. Możliwość wykorzystywania 64 procesorów wirtualnych oraz 1TB pamięci RAM i dysku o pojemności do 64TB przez każdy wirtualny serwerowy system operacyjny.
3. Możliwość budowania klastrów składających się z 64 węzłów, z możliwością uruchamiania 7000 maszyn wirtualnych.
4. 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.
5. Wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany pamięci RAM bez przerywania pracy.
6. Wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany procesorów bez przerywania pracy.
7. Automatyczna weryfikacja cyfrowych sygnatur sterowników w celu sprawdzenia, czy sterownik przeszedł testy jakości przeprowadzone przez producenta systemu operacyjnego.
8. Możliwość dynamicznego obniżania poboru energii przez rdzenie procesorów niewykorzystywane w bieżącej pracy. Mechanizm ten musi uwzględniać specyfikę procesorów wyposażonych w mechanizmy Hyper-Threading.
9. Wbudowane wsparcie instalacji i pracy na wolumenach, które:
   a) pozwalają na zmianę rozmiaru w czasie pracy systemu,
   b) umożliwiają tworzenie w czasie pracy systemu migawek, dających użytkownikom końcowym (lokalnym i sieciowym) prosty wgląd w poprzednie wersje plików i folderów,
   c) umożliwiają kompresję "w locie" dla wybranych plików i/lub folderów,
   d) umożliwiają zdefiniowanie list kontroli dostępu (ACL).
10. Wbudowany mechanizm klasyfikowania i indeksowania plików (dokumentów) w oparciu o ich zawartość.

11. Wbudowane szyfrowanie dysków przy pomocy mechanizmów posiadających certyfikat FIPS 140-2 lub równoważny wydany przez NIST lub inną agendę rządową zajmującą się bezpieczeństwem informacji.
12. Możliwość uruchamiania aplikacji internetowych wykorzystujących technologię ASP.NET
13. Możliwość dystrybucji ruchu sieciowego HTTP pomiędzy kilka serwerów.
14. Wbudowana zapora internetowa (firewall) z obsługą definiowanych reguł dla ochrony połączeń internetowych i intranetowych.
15. Dostępne dwa rodzaje graficznego interfejsu użytkownika:
    a) klasyczny, umożliwiający obsługę przy pomocy klawiatury i myszy,
    b) dotykowy umożliwiający sterowanie dotykiem na monitorach dotykowych.
16. Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, przeglądarka internetowa, pomoc, komunikaty systemowe,
17. Możliwość zmiany języka interfejsu po zainstalowaniu systemu, dla co najmniej 10 języków poprzez wybór z listy dostępnych lokalizacji.
18. Mechanizmy logowania w oparciu o:
    a) Login i hasło,
    b) Karty z certyfikatami (smartcard),
    c) Wirtualne karty (logowanie w oparciu o certyfikat chroniony poprzez moduł TPM),
19. Możliwość wymuszania wieloelementowej dynamicznej kontroli dostępu dla: określonych grup użytkowników, zastosowanej klasyfikacji danych, centralnych polityk dostępu w sieci, centralnych polityk audytowych oraz narzuconych dla grup użytkowników praw do wykorzystywania szyfrowanych danych..
20. Wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug&Play).
21. Możliwość zdalnej konfiguracji, administrowania oraz aktualizowania systemu.
22. Dostępność bezpłatnych narzędzi producenta systemu umożliwiających badanie i wdrażanie zdefiniowanego zestawu polityk bezpieczeństwa.
23. Pochodzący od producenta systemu serwis zarządzania polityką dostępu do informacji w dokumentach (Digital Rights Management).
24. Wsparcie dla środowisk Java i .NET Framework 4.x – możliwość uruchomienia aplikacji działających we wskazanych środowiskach.
25. Możliwość implementacji następujących funkcjonalności bez potrzeby instalowania dodatkowych produktów (oprogramowania) innych producentów wymagających dodatkowych licencji:
    a) Podstawowe usługi sieciowe: DHCP oraz DNS wspierający DNSSEC,
    b) Usługi katalogowe oparte o LDAP i pozwalające na uwierzytelnianie użytkowników stacji roboczych, bez konieczności instalowania dodatkowego oprogramowania na tych stacjach, pozwalające na zarządzanie zasobami w sieci (użytkownicy, komputery, drukarki, udziały sieciowe), z możliwością wykorzystania następujących funkcji:
        - Podłączenie do domeny w trybie offline – bez dostępnego połączenia sieciowego z domeną,

- Ustanawianie praw dostępu do zasobów domeny na bazie sposobu logowania użytkownika – na przykład typu certyfikatu użytego do logowania,
- Odzyskiwanie przypadkowo skasowanych obiektów usługi katalogowej z mechanizmu kosza.
- Bezpieczny mechanizm dołączania do domeny uprawnionych użytkowników prywatnych urządzeń mobilnych opartych o iOS i Windows 8.1.

c) Zdalna dystrybucja oprogramowania na stacje robocze.

d) Praca zdalna na serwerze z wykorzystaniem terminala (cienkiego klienta) lub odpowiednio skonfigurowanej stacji roboczej

e) Centrum Certyfikatów (CA), obsługa klucza publicznego i prywatnego) umożliwiające:
- Dystrybucję certyfikatów poprzez http
- Konsolidację CA dla wielu lasów domeny,
- Automatyczne rejestrowania certyfikatów pomiędzy różnymi lasami domen,
- Automatyczne występowanie i używanie (wystawianie) certyfikatów PKI X.509.

f) Szyfrowanie plików i folderów.

g) Szyfrowanie połączeń sieciowych pomiędzy serwerami oraz serwerami i stacjami roboczymi (IPSec).

h) Możliwość tworzenia systemów wysokiej dostępności (klastry typu fail-over) oraz rozłożenia obciążenia serwerów.

i) Serwis udostępniania stron WWW.

j) Wsparcie dla protokołu IP w wersji 6 (IPv6),

k) Wsparcie dla algorytmów Suite B (RFC 4869),

l) Wbudowane usługi VPN pozwalające na zestawienie nielimitowanej liczby równoczesnych połączeń i niewymagające instalacji dodatkowego oprogramowania na komputerach z systemem Windows,

m) budowane mechanizmy wirtualizacji (Hypervisor) pozwalające na uruchamianie do 1000 aktywnych środowisk wirtualnych systemów operacyjnych. Wirtualne maszyny w trakcie pracy i bez zauważalnego zmniejszenia ich dostępności mogą być przenoszone pomiędzy serwerami klastra typu failover z jednoczesnym zachowaniem pozostałej funkcjonalności. Mechanizmy wirtualizacji mają zapewnić wsparcie dla:
- Dynamicznego podłączania zasobów dyskowych typu hot-plug do maszyn wirtualnych,
- Obsługi ramek typu jumbo frames dla maszyn wirtualnych.
- Obsługi 4-KB sektorów dysków
- Nielimitowanej liczby jednocześnie przenoszonych maszyn wirtualnych pomiędzy węzłami klastra
- Możliwości wirtualizacji sieci z zastosowaniem przełącznika, którego funkcjonalność może być rozszerzana jednocześnie poprzez oprogramowanie kilku innych dostawców poprzez otwarty interfejs API.
- Możliwości kierowania ruchu sieciowego z wielu sieci VLAN bezpośrednio do pojedynczej karty sieciowej maszyny wirtualnej (tzw. trunk mode)

26. Możliwość automatycznej aktualizacji w oparciu o poprawki publikowane przez producenta wraz z dostępnością bezpłatnego rozwiązania producenta serwerowego systemu operacyjnego umożliwiającego lokalną dystrybucję poprawek zatwierdzonych przez administratora, bez połączenia z siecią Internet. 27. Wsparcie dostępu do zasobu dyskowego poprzez wiele ścieżek (Multipath). 28. Możliwość instalacji poprawek poprzez wgranie ich do obrazu instalacyjnego. 29. Mechanizmy zdalnej administracji oraz mechanizmy (również działające zdalnie) administracji przez skrypty. 30. Możliwość zarządzania przez wbudowane mechanizmy zgodne ze standardami WBEM oraz WS-Management organizacji DMTF.

12. LICENCJE NA OPROGRAMOWANIE DO REALIZACJI KOPII ZAPASOWYCH

MINIMALNE WYMAGANIA FUNKCJONALNE, TECHNICZNE, UŻYTKOWE, JAKOŚCIOWE
1. W ramach licencji wieczystej (bezterminowej) oprogramowanie musi zapewnić realizację kopii zapasowych z 1 (jednego) serwera fizycznego i 4 (czterech) maszyn wirtualnych. 2. Wykonawca zapewnieni wsparcie techniczne (support producenta) dla dostarczonego oprogramowania przez okres 1 roku (12 miesięcy) lecz nie dłużej niż do 30.09.2023 r. 3. Zamawiający wymaga określenia przez oferenta w formularzu ofertowym co najmniej następujących cech oferowanego oprogramowania: producent (marka), model (symbol), wersji, typ licencji oraz liczba licencji. 4. Oprogramowanie musi współpracować z infrastrukturą VMware w wersji 5.5, 6.0, 6.5, 6.7 and 7.0 oraz Microsoft Hyper-V 2008R2SP1, 2012, 2012 R2, 2019 i 2022. Wszystkie funkcjonalności w specyfikacji muszą być dostępne na wszystkich wspieranych platformach wirtualizacyjnych, chyba, że wyszczególniono inaczej. 5. Oprogramowanie musi współpracować z hostami zarządzanymi przez VMware vCenter oraz pojedynczymi hostami. 6. Oprogramowanie musi współpracować z hostami zarządzanymi przez System Center Virtual Machine Manger, klastrami hostów oraz pojedynczymi hostami. 7. 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 pozwalać na tworzenie kopii zapasowych w trybach: Pełny, pełny

syntetyczny, przyrostowy i odwrotnie przyrostowy (tzw. reverse-inremental)

4. 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.
5. 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.
6. 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 takiej puli.
7. Oprogramowanie musi pozwalać na rozszerzenie lokalnej przestrzeni backupowej poprzez integrację z Microsoft Azure Blob, Amazon S3 oraz z innymi kompatybilnymi z S3 macierzami obiektowymi. Proces migracji danych powinien być zautomatyzowany. Jedynie unikalne bloki mogą być przesyłane w celu oszczędności pasma oraz przestrzeni na przechowywane dane. Funkcjonalność ta nie może mieć wpływu na możliwości odtwarzania danych.
8. Oprogramowanie nie może instalować żadnych stałych agentów wymagających wdrożenia czy upgradowania wewnątrz maszyny wirtualnej dla jakichkolwiek funkcjonalności backupu lub odtwarzania
9. Oprogramowanie musi mieć możliwość uruchamiania dowolnych skryptów przed i po zadaniu backupowym lub przed i po wykonaniu zadania snapshota.
10. Oprogramowanie musi oferować portal samoobsługowy, umożliwiający odtwarzanie użytkownikom wirtualnych maszyn, obiektów MS Exchange i baz danych MS SQL oraz Oracle (w tym odtwarzanie point-in-time)
11. Oprogramowanie musi zapewniać możliwość delegacji uprawnień do odtwarzania na portalu
12. Oprogramowanie musi mieć możliwość integracji z innymi systemami poprzez wbudowane RESTful API
13. Oprogramowanie musi mieć wbudowane mechanizmy backupu konfiguracji w celu prostego odtworzenia systemu po całkowitej reinstalacji.
14. 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.
15. Oprogramowanie musi posiadać mechanizmy chroniące przed utratą hasła szyfrowania.
16. Oprogramowanie musi wspierać backup maszyn wirtualnych używających współdzielonych dysków VHDX na Hyper-V (shared VHDX)
17. Oprogramowanie musi posiadać architekturę klient/serwer z możliwością instalacji wielu instancji konsoli administracyjnych

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 mechnizmy 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.
4. Oprogramowanie musi oferować ten mechanizm z dokładnością do pojedynczego datastoru.
5. Oprogramowanie musi automatycznie wykrywać i usuwać snapshoty-sieroty (orphaned snapshots), które mogą zakłócić poprawne wykonanie backupu. Proces ten nie może wymagać interakcji administratora.
6. Oprogramowanie musi wspierać kopiowanie backupów na taśmy wraz z pełnym śledzeniem wirtualnych maszyn
7. Oprogramowanie musi posiadać wsparcie dla NDMP
8. Oprogramowanie musi mieć możliwość tworzenia retencji GFS (Grandfather-Father-Son)
9. Oprogramowanie musi umieć korzystać z protokołu DDBOOST w przypadku, gdy repozytorium backupów jest umiejscowione na Dell EMC DataDomain. Funkcjonalność powinna wspierać łącze sieciowe lub FC.
10. Oprogramowanie musi umieć korzystać z protokołu Catalyst (w tym Catalyst Copy) w przypadku, gdy repozytorium backupów jest umiejscowione na HPE StoreOnce. Funkcjonalność powinna wspierać łącze sieciowe lub FC.
11. Oprogramowanie musi wspierać BlockClone API w przypadku użycia Windows Server 2016 lub 2019 z systemem pliku ReFS jako repozytorium backupu. Podobna funkcjonalność musi być zapewniona dla repozytoriów opartych o linuxowy system plików XFS.
12. Repozytoria oparte o XFS muszą pozwalać na zmiezmienność danych przez określoną ilość czasu (tzw Immutability)
13. Oprogramowanie musi mieć możliwość kopiowania backupów oraz replikacji wirtualnych maszyn z wykorzystaniem wbudowanej akceleracji WAN.
14. 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.
15. Oprogramowanie musi mieć możliwość replikacji ciągłej, opartej o VMware VAIO, włączonych wirtualnych maszyn bezpośrednio z infrastruktury VMware vSphere. Dla replikacji ciągłej musi być możliwośc zdefiniowania dziennika pozwalającego na odzyskanie danych z dowolnego punku w ramach ustalonego parametru RPO.
16. Oprogramowanie musi umożliwiać przechowywanie punktów przywracania dla replik
17. Oprogramowanie musi umożliwiać wykorzystanie istniejących w infrastrukturze wirtualnych maszyn jako źródła do dalszej replikacji (replica seeding)

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 oraz Hyper-V niezależnie od rodzaju storage'u użytego do przechowywania kopii zapasowych.
2. Dodatkowo dla środowiska vSphere i Hyper-V 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 umożliwiać pełne odtworzenie wirtualnej maszyny, plików konfiguracji i dysków.
6. Oprogramowanie musi umożliwiać pełne odtworzenie wirtualnej maszyny bezpośrednio do Microsoft Azure, Microsoft Azure Stack oraz Amazon EC2.
7. Oprogramowanie musi umożliwić odtworzenie plików 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.
8. Oprogramowanie musi mieć możliwość odtworzenia plików bezpośrednio do maszyny wirtualnej poprzez sieć, przy pomocy VIX API dla platformy VMware i PowerShell Direct dla platformy Hyper-V.
9. Oprogramowanie musi wspierać odtwarzanie pojedynczych plików z następujących systemów plików:
   a. Linux: ext2, ext3, ext4, ReiserFS, JFS, XFS, Btrfs
   b. BSD: UFS, UFS2
   c. Solaris: ZFS, UFS
   d. Mac: HFS, HFS+
   e. Windows: NTFS, FAT, FAT32, ReFS
   f. Novell OES: NSS
10. Oprogramowanie musi wspierać przywracanie plików z partycji Linux LVM oraz Windows Storage Spaces.
11. Oprogramowanie musi umożliwiać szybkie granularne odtwarzanie obiektów aplikacji bez użycia jakiegokolwiek agenta zainstalowanego wewnątrz maszyny wirtualnej.
12. Oprogramowanie musi wspierać granularne odtwarzanie obiektów Active Directory takich jak konta komputerów, konta użytkowników oraz pozwalać na odtworzenie haseł.
13. Oprogramowanie musi wspierać granularne odtwarzanie dowolnych atrybutów, rekordów DNS zintegrowanych z AD, Microsoft System Objects, certyfikatów CA oraz elementów AD Sites.
14. Oprogramowanie musi wspierać granularne odtwarzanie Microsoft Exchange 2010 i nowszych (dowolny obiekt w tym obiekty w folderze "Permanently Deleted Objects").

15. Oprogramowanie musi wspierać przywracanie danych Exchange do oryginalnego środowiska.
16. Oprogramowanie musi wspierać granularne odtwarzanie Microsoft SQL 2005 i nowszych
17. Oprogramowanie musi wspierać odtworzenie point-in-time wraz z możliwością przywrócenia bazy do oryginalnego środowiska.
18. Oprogramowanie musi wspierać granularne odtwarzanie Microsoft Sharepoint 2010 i nowszych.
19. Oprogramowanie musi wspierać odtworzenia elementów, witryn, uprawnień dla witryn Sharepoint.
20. 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.
21. Oprogramowanie musi pozwalać na zaprezentowanie oraz migrację online baz MS SQL oraz Oracle bezpośrednio z pliku kopii zapasowej do działającego serwera bazodanowego.
22. Oprogramowanie musi posiadać natywną integrację dla backupów wykonywanych poprzez Oracle RMAN
23. Oprogramowanie musi posiadać natywną integrację dla backupów wykonywanych poprzez SAP HANA
24. 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.
2. Dla VMware'a oprogramowanie musi pozwalać na uruchomienie takiego środowiska 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 mieć podobne mechanizmy dla replik w środowisku vSphere.
5. 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.
6. Oprogramowanie musi umożliwiać dwuetapowe, automatyczne, odtwarzanie maszyn wirtualnych z możliwością wstrzyknięcia dowolnego skryptu przed odtworzeniem danych do środowiska produkcyjnego.

Monitoring

1. System musi zapewnić możliwość monitorowania środowiska wirtualizacyjnego opartego na

VMware vSphere i Microsoft Hyper-V bez potrzeby korzystania z narzędzi firm trzecich
2. System musi umożliwiać monitorowanie środowiska wirtualizacyjnego VMware w wersji 5.5, 6.0, 6.5, 6.7 and 7.0 - zarówno w bezpłatnej wersji ESXi jak i w pełnej wersji ESX/ESXi zarządzane przez konsole vCenter Server lub pracujące samodzielnie.
3. System musi umożliwiać monitorowanie środowiska wirtualizacyjnego Microsoft Hyper-V 2008 R2 SP1, 2012, 2012 R2, 2016 oraz 2019 zarówno w wersji darmowej jak i zawartej w płatnej licencji Microsoft Windows Server zarządzane poprzez System Center Virtual Machine Manager lub pracujące samodzielnie.
4. System musi mieć status „VMware Ready" i być przetestowany i certyfikowany przez Vmware.
5. System musi umożliwiać kategoryzacje obiektów infrastruktury wirtualnej niezależnie od hierarchii stworzonej w vCenter.
6. System musi umożliwiać tworzenie alarmów dla całych grup wirtualnych maszyn jak i pojedynczych wirtualnych maszyn.
7. System musi dawać możliwość układania terminarza raportów i wysyłania tych raportów przy pomocy poczty elektronicznej w formacie HTML oraz Excel.
8. System musi dawać możliwość podłączenia się do kilku instancji vCenter Server i serwerów Hyper-V jednocześnie, w celu centralnego monitorowania wielu środowisk.
9. System musi mieć wbudowane predefiniowane zestawy alarmów wraz z możliwością tworzenia własnych alarmów i zdarzeń przez administratora.
10. System musi mieć wbudowane połączenie z bazą wiedzy opisującą problemy z predefiniowanych alarmów.
11. System musi mieć centralną konsolę z sumarycznym podglądem wszystkich obiektów infrastruktury wirtualnej (ang. Dashboard).
12. System musi mieć możliwość monitorowania platformy sprzętowej, na której jest zainstalowana infrastruktura wirtualna.
13. System musi zapewnić możliwość podłączenia się do wirtualnej maszyny (tryb konsoli) bezpośrednio z narzędzia monitorującego.
14. System musi mieć możliwość integracji z oprogramowaniem do tworzenia kopii zapasowych tego samego producenta.
15. System musi mieć możliwość monitorowania obciążenia serwerów backupowych, ilości zabezpieczanych danych oraz statusu zadań kopii zapasowych, replikacji oraz weryfikacji odzyskiwalności maszyn wirtualnych.
16. System musi oferować inteligentną diagnostykę rozwiązania backupowego poprzez monitorowanie logów celem wykrycia znanych problemów oraz błędów konfiguracyjnych w celu wskazania rozwiązania bez potrzeby otwierania zgłoszenia suportowego oraz bez potrzeby wysyłania jakichkolwiek danych diagnostycznych do producenta oprogramowania backupu.
17. System musi mieć możliwość granularnego monitorowania infrastruktury, zależnego od uprawnień nadanym użytkownikom dla platformy Vmware.
18. System musi mieć możliwość monitorowania instancji VMware vCloud Director w wersji 8.x i 9.x.

Raportowanie

1. System raportowania musi umożliwić tworzenie raportów z infrastruktury wirtualnej bazującej na VMware ESX/ESXi 5.5, 6.0, 6.5, 6.7 and 7.0 vCenter Server 5.x oraz 6.x jak również Microsoft Hyper-V 2008 R2 SP1, 2012, 2012 R2, 2016 oraz 2019
2. System musi wspierać wiele instancji vCenter Server i Microsoft Hyper-V jednocześnie bez konieczności instalowania dodatkowych modułów.
3. System musi być certyfikowany przez VMware i posiadać status „VMware Ready".
4. System musi być systemem bezagentowym. Nie dopuszcza się możliwości instalowania przez system agentów na monitorowanych hostach ESXi i Hyper-V.
5. System musi mieć możliwość eksportowania raportów do formatów Microsoft Word, Microsoft Excel, Microsoft Visio, Adobe PDF.
6. System musi mieć możliwość ustawienia harmonogramu kolekcji danych z monitorowanych systemów jak również możliwość tworzenia zadań kolekcjonowania danych ad-hoc.
7. System musi mieć możliwość ustawienia harmonogramu generowania raportów i dostarczania ich do odbiorców w określonych przez administratora interwałach.
8. System w raportach musi mieć możliwość uwzględniania informacji o zmianach konfiguracji monitorowanych systemów.
9. System musi mieć możliwość generowania raportów z dowolnego punktu w czasie zakładając, że informacje z tego czasu nie zostały usunięte z bazy danych.
10. System musi posiadać predefiniowane szablony z możliwością tworzenia nowych jak i modyfikacji wbudowanych.
11. System musi mieć możliwość analizowania „przeszacowanych" wirtualnych maszyn wraz z sugestią zmian w celu optymalnego wykorzystania fizycznej infrastruktury.
12. System musi mieć możliwość generowania raportów na podstawie danych uzyskanych z oprogramowania do tworzenia kopii zapasowych tego samego producenta.
13. System musi mieć możliwość generowania raportu dotyczącego zabezpieczanych maszyn, zdefiniowanych zadań tworzenia kopii zapasowych oraz replikacji jak również wykorzystania zasobów serwerów backupowych.
14. System musi mieć możliwość generowania raportu planowania pojemności (capacity planning) bazującego na scenariuszach 'what-if".
15. System musi mieć możliwość granularnego raportowania infrastruktury, zależnego od uprawnień nadanym użytkownikom dla platformy Vmware.
16. System musi mieć możliwość generowania raportów dotyczących tzw. migawek-sierot (orphaned snapshots).
17. System musi mieć możliwość generowania personalizowanych raportów zawierających informacje z dowolnych predefiniowanych raportów w pojedynczym dokumencie.

Agent

1. Rozwiązanie musi wykonywać kopię zapasową systemu Windows oraz Linux wykorzystując agenta znajdującego się wewnątrz systemu operacyjnego
2. Rozwiązanie musi wspierać systemy operacyjne Windows w wersjach klienckich oraz serwerowych
3. Rozwiązanie musi wspierać co najmniej następujące dystrybucje systemów Linux:

- Debian, Ubuntu, RHEL, CentOS, Oracle Linux, SLES, Fedora, openSUSE

4. Rozwiązanie musi wspierać systemy operacyjne macOS
5. Rozwiązanie musi wspierać wykonywanie kopi zapasowych następujących systemów plików:
   - NTFS, ReFS, FAT32, ext2, ext3, ext4, ReiserFS, JFS, XFS, F2FS, Brtfs (dla kernela 3.16 i nowszych), APFS, HFS, HFS+, NILFS2
6. Rozwiązanie musi mieć możliwość instalacji oraz zarządzania wykorzystując tryb niezależny (per agent) jak również zcentralizowany (poprzez centralną konsolę zarządzającą)
7. Rozwiązanie musi wspierać systemy oparte o Microsoft Failover Cluster
8. Rozwiązanie musi wspierać zabezpieczanie do oraz odzyskiwanie z urządzeń blokowych pozwalając na odzysk całej maszyny (tzw. bare metal recovery) wybranych wolumenów, oraz wybranych plików i folderów
9. Rozwiązanie musi wspierać backup podłączonych dysków USB
10. Kopia zapasowa całej maszyny oraz pojedynczych wolumenów musi być wykonywana na poziomie blokowym
11. Rozwiązanie musi pozwalać na przechowywanie kopii zapasowych na:
    - Lokalnych (wewnętrznych) dyskach zabezpieczanej maszyny
    - Direct Attached Storage (DAS), takich jak zewnętrzne dyski USB, eSATA lub Firewire
    - Network Attached Storage (NAS) pozwalającym na wystawienie swoich zasobów poprzez SMB (CIFS) lub NFS.
    - Zcentralizowanym repozytorium danych
    - Bezpośrednio na zasobach Chmury
12. Rozwiązanie musi wspierać deduplikacje oraz kompresję na źródle. Dane wysyłane na repozytorium muszą być już odpowiednio przetworzone
13. Rozwiązanie musi wspierać kontrolę pasma sieciowego
14. Rozwiązanie musi wspierać ograniczenie wykonywania backupów dla konkretnych sieci bezprzewodowych
15. Rozwiązanie musi wspierać ograniczenia wykonywania backupów dla połączeń VPN
16. Rozwiązanie musi wspierać śledzenie zmienionych bloków podczas wykonywania blokowych kopii zapasowych. Dla systemów Windows technologia śledzenia bloków dla systemów serwerowych musi być certyfikowana przez Microsoft
17. Rozwiązanie musi wspierać skrypty wykonywane przed i po wykonaniu zadania oraz przed i po wykonaniu migawki na poziomie wolumenu.
18. Rozwiązanie musi wspierać technologię BitLocker
19. Rozwiązanie musi wspierać uruchamianie z nośnika odtwarzania
20. Rozwiązanie musi wspierać odzysk pojedynczych elementów aplikacji z jednoprzebiegowej kopii zapasowej dla:
    - Microsoft Exchange 2010 i nowszych
    - Microsoft Active Directory 2003 i nowszych
    - Microsoft Sharepoint 2010 i nowszych
    - Microsoft SQL 2005 i nowszych
    - Oracle 11g i nowszych
21. Rozwiązanie musi wspierać odzysk do konkretnego punktu w czasie (point-in-time) dla

wspieranych systemów bazodanowych
22. Rozwiązanie musi umożliwiać natychmiastowe publikowanie baz MS SQL poprzez bezpośrednie uruchomienie ich z pliku backupu.
23. Rozwiązanie musi wspierać odzysk obrazów kopii zapasowych bezpośrednio do Microsoft Azure, Microsoft Azure Stack oraz Amazon EC2
24. Rozwiązanie musi wspierać szyfrowanie
25. Rozwiązanie musi wspierać możliwość wykonywania kopii zapasowych stacji klienckich, lokalnie do repozytorium tymczasowego (cache) gdy połączenie sieciowe do głównego repozytorium kopii zapasowych jest niedostępne
26. Rozwiązanie musi posiadać funkcjonalność automatycznego zmniejszenia szybkości przetwarzania danych, aby nie dopuścić do obniżenia wydajności systemu zabezpieczanego
27. Rozwiązanie musi posiadać ochronę przed ransomware poprzez automatyczne odmontowanie nośnika po wykonanym backupie stacji klienckiej
28. Rozwiązanie musi wspierać tworzenie wielu zadań backupowych.

13. USŁUGI INFORMATYCZNE Z ZAKRESU WDROŻENIA KONSERWACJI I SERWISU SPRZĘTU INFORMATYCZNEGO ORAZ OPROGRAMOWANIA

ATRYBUT	MINIMALNE WYMAGANIA FUNKCJONALNE, TECHNICZNE, UŻYTKOWE, JAKOŚCIOWE
Usługi	Celem prac jest przygotowanie środowiska teleinformatycznego, na potrzeby realizacji projektu, zbudowanego w oparciu o dostarczone urządzenia sprzętowe i oprogramowanie opisane w podmiotowym dokumencie. Zamawiający umożliwi Wykonawcy dostęp do infrastruktury w ustalonym wcześniej terminie w celu dokonania analizy i przygotowania procedur wdrożenia, migracji do nowego środowiska. Dostęp do infrastruktury będzie możliwy pod nadzorem Zamawiającego i po spełnieniu warunków wynikających z Polityki Bezpieczeństwa. Po zapoznaniu się z architekturą sieciową urzędu Wykonawca przedstawi plan reorganizacji sieci oraz wirtualizacji z uwzględnieniem istniejącego i dostarczanego sprzętu. Schemat ten musi być uzgodniony z Zamawiającym i uwzględniać jego wytyczne. Zamawiający udzieli Wykonawcy wszelkich niezbędnych informacji niezbędnych do przeprowadzenia wdrożenia. **W ramach oferty Zamawiający wymaga przeprowadzenia wdrożenia na zasadach projektowych.**

	Zamawiający wymaga sporządzenia Planu Wdrożenia uwzględniającego fakt wykonania wdrożenia bez przerywania bieżącej działalności Zamawiającego oraz przewidującego rozwiązania dla sytuacji kryzysowych wdrożenia. Odbiór wdrożenia nastąpi na podstawie zgodności stanu faktycznego z Dokumentacją Powykonawczą.
Montaż i fizyczne uruchomienie systemu	Zamawiający wymaga zainstalowania całości dostarczonego rozwiązania w pomieszczeniu serwerowni, jak i innych wskazanych miejscach co najmniej w zakresie: 1. Wniesienie, ustawienie i fizyczny montaż wszystkich dostarczonych urządzeń i szafy w dostarczonej i zainstalowanej szafie Rack 42U w pomieszczeniu (miejscu) wskazanym przez Zamawiającego. 2. Urządzenia, które nie są montowane w szafie teleinformatycznej np.: komputery, powinny zostać zamontowane w miejscach wskazanych przez Zamawiającego oraz skonfigurowane i dołączone do infrastruktury Zamawiającego. 3. Usunięcie opakowań i innych zbędnych pozostałości po procesie instalacji urządzeń. 4. Podłączenie całości rozwiązania do infrastruktury Zamawiającego. 5. Wykonanie procedury aktualizacji firmware dostarczonych elementów do najnowszej wersji oferowanej przez producenta sprzętu. 6. Dla urządzeń modularnych wymagany jest montaż i instalacja wszystkich podzespołów. 7. Wykonanie połączeń kablowych pomiędzy dostarczonymi urządzeniami w celu zapewnienia komunikacji - Wykonawca musi zapewnić niezbędne okablowanie (np.: patchordy miedziane kat. 6 UTP lub światłowodowe uwzględniające typ i model interfejsu w urządzeniu sieciowym). 8. Demontaż „starych” urządzeń IT z szaf teleinformatycznych, które nie będą już wykorzystywane. 9. Po wykonaniu instalacji wymagane jest przeprowadzenie testów sprawdzających poprawność instalacji i działania urządzeń. 10. Wykonawca musi przeprowadzić instalację UPS wraz z testami zasilania.
Konfiguracja przełączników sieci LAN	Zamawiający wymaga stworzenia połączeń sieciowych pomiędzy wszystkimi wskazanymi urządzeniami sieciowymi. Centralnym punktem będzie serwerownia zlokalizowana w urzędzie gminy (Miejsce instalacji przełączników sieci LAN). Przełączniki będą stanowił centralny punkt wymiany danych sieciowych z punktu widzenia warstwy drugiej modelu ISO/OSI.

	1. Konfiguracja dostarczanych przełączników w zakresie: a. Aktualizacja oprogramowania układowego do najnowszej stabilnej wersji oferowanej przez producenta urządzenia. b. Konfiguracja sieci wirtualnych VLAN, taka liczba sieci wirtualnych aby odseparować różne typy ruchu, w porozumieniu z zamawiającym. c. Konfiguracja połączeń pomiędzy istniejącymi przełącznikami z wykorzystaniem połączeń światłowodowych lub miedzianych (gdzie to jest możliwe, utworzenie agregacji na wspieranych urządzeniach). d. Konfiguracja routingu pomiędzy sieciami VLAN na firewall'u. e. Testowanie obsługi ruchu sieciowego. f. Testowanie skuteczności zabezpieczeń
Konfiguracja elementów bezpieczeństwa sieciowego.	Urządzenie firewall Wykonawca skonfiguruje w zakresie min.: 1. Aktualizacja oprogramowania układowego do najnowszej stabilnej wersji oferowanej przez producenta urządzenia. 2. Aktywacja (jeśli wymagana) urządzenia na stronie internetowej producenta. 3. Aktywacja (jeśli wymagana) funkcjonalności oferowanych przez urządzenia (AV, IPS, Kontrola Aplikacji, Filtrowanie WWW, Filtrowanie Email) 4. Przygotowanie projektu włączenia urządzenia do sieci LAN urzędu gminy 5. Konfiguracja dostarczonego systemu Firewall: a. Konfiguracja podstawowych parametrów b. Konfiguracja translacji adresów NAT c. Konfiguracja mechanizmów ochrony wybranych sieci VLAN, do których przyłączone zostaną np. serwery, serwery komunikacyjne telefonii IP, itp. d. Konfiguracja inspekcji określonych protokołów sieciowych; e. Konfiguracja reguł dostępu do określonych podsieci, chronionych przez moduł Firewall; f. Konfiguracja zarządzania Firewall przez dedykowaną stację zarządzającą bezpieczeństwem sieciowym; g. Testowanie działania bramy 6. Konfiguracja modułów należących do systemu wykrywania włamań IPS: a. Konfiguracja podstawowych parametrów b. Konfiguracja mechanizmów ochrony określonych sieci VLAN przez moduł wykrywania włamań;

	c. Konfiguracja reguł kontroli ruchu sieciowego przez moduły oraz sposobów reakcji na pojawienie się niepożądanego ruchu sieciowego; d. Konfiguracja zarządzania modułami przez dedykowaną stację zarządzającą bezpieczeństwem sieciowym; e. Testowanie działania ochrony IPS 7. Konfiguracja modułu ochrony antywirusowej, antyspyware, blokowania transferu plików, antyspamowa, filtrowania i blokowania odwołań do niepożądanych adresów URL. a. Przypisanie adresu IP do zarządzania. b. Konfiguracja inspekcji protokołów HTTP, SMTP, FTP, POP3 c. Definicja reguł filtrowania/blokowania 8. Konfiguracja tuneli SSL VPN celem zapewnienia bezpiecznego dostępu do sieci wewnętrznej z uwierzytelnieniem w oparciu o usługę katalogową. 9. Uruchomienie i skonfigurowanie instancji systemu bezpieczeństwa dla skonfigurowanych sieci wirtualnych VLAN, taka liczba sieci wirtualnych aby odseparować różne typy ruchu, w porozumieniu z Zamawiającym. 10. W instancji systemu bezpieczeństwa należy skonfigurować co najmniej 3 profile (wytyczne przekaże Zamawiający) dla każdej z poniższych funkcjonalności: a. kontrola dostępu - zapora ogniowa klasy Statless Inspection b. ochrona przed wirusami – antywirus [AV] (dla protokołów SMTP, POP3, IMAP, HTTP, FTP, HTTPS) umożliwiający skanowanie wszystkich rodzajów plików, w tym zip, rar c. ochrona przed atakami - Intrusion Prevention System [IPS/IDS] d. kontrola stron internetowych pod kątem rozpoznawania witryn potencjalnie niebezpiecznych: zawierających złośliwe oprogramowanie, stron szpiegujących oraz udostępniających treści typu SPAM. e. kontrola zawartości poczty – antyspam [AS] (dla protokołów SMTP, POP3, IMAP) f. kontrola pasma oraz ruchu [QoS, Traffic shaping] g. Kontrola aplikacji oraz rozpoznawanie ruchu P2P h. Filtra WWW (w oparciu o kategorie stron WWW oraz własną bazę URL) i. Inspekcja ruchu SSL j. Ochrony przez atakami na stacje klienckie k. Kontrola pasma 11. Konfiguracja logowania i raportowania.

	12. Konfiguracja logowania i raportowania do alternatywnego serwera SYSLOG uruchomionego na serwerze NAS (instalacja i konfiguracja serwera SYSLOG spoczywa na Wykonawcy). Jeśli dla zapewnienia tej funkcjonalności wymagane są jakiekolwiek licencje – ich dostarczenie spoczywa na Wykonawcy.
Instalacja i konfiguracja serwera, instalacja systemu operacyjnego serwera	Zamawiający wymaga wykonania fizycznej instalacji serwera o którym mowa w punkcie 5 we wskazanej szafie Rack oraz: 1. Przygotowania konfiguracji odpowiedniego poziomu RAID wskazaną przez Zamawiającego. 2. Instalacji systemów operacyjnych oraz ich aktywacji 3. Instalacji niezbędnych aktualizacji oraz poprawek związane z bezpieczeństwem udostępnionych przez producenta systemu operacyjnego
Wirtualizacja	Zamawiający wymaga zaplanowania, uruchomienia oraz przetestowania środowiska wirtualizacyjnego, co najmniej w zakresie: 1. Przygotowanie serwera do instalacji oprogramowania wirtualizacyjnego. 2. Aktualizacji oprogramowania układowego do najnowszej stabilnej wersji oferowanej przez producenta. 3. Instalacji oprogramowania wirtualizacyjnego na instalowanym serwerze. 4. Instalacji oprogramowania do zarzadzania środowiskiem wirtualizacyjnym. 5. Instalacji najnowszych poprawek do środowiska wirtualizacyjnego oferowanych przez producenta oprogramowania wirtualizacyjnego oraz przez producenta serwerów. 6. Konfiguracji sieci w infrastrukturze wirtualnej - konieczna jest konfiguracja wspierająca wirtualne sieci LAN w oparciu o protokół 802.1q. 7. Przygotowania koncepcji i wykonania wirtualizacji do 4 wirtualnych maszyn. Z przeniesieniem systemów używanych w UG. 8. Instalacji i konfiguracji oprogramowania zarządzającego środowiskiem wirtualnym. 9. Migracji istniejącej infrastruktury fizycznej do środowiska wirtualnego 10. Konfiguracji uprawnień w środowisku wirtualizacyjnym - integracja z usługą katalogową.
Uruchomienie usługi katalogowej oraz niezbędnych komponentów,	Uruchomienie usługi katalogowej, komponentów odpowiedzialnych za rozwiązywanie nazw. Usługa katalogowa musi być uruchomiona na serwerze wraz z komponentami odpowiedzialnymi za rozwiązywanie nazw. Należy szczególną uwagę zwrócić na poprawne funkcjonowanie mechanizmów replikacji. Usługę katalogową należy skonfigurować w taki

migracja danych do usługi katalogowej	sposób, aby możliwe było wykorzystanie możliwie wszystkich funkcjonalności oferowanych przez zastosowany system operacyjny, a w szczególności możliwość skonfigurowania różnych polityk haseł dla różnych grup zabezpieczeń, możliwość łatwego odzyskania usuniętego obiektu usługi katalogowej wraz ze wszystkimi danymi, jakie były z nimi związane przed usunięciem. Utworzenie struktury jednostek organizacyjnych na podstawie schematu organizacyjnego dostarczonego przez Zamawiającego. Zamawiający wymaga skonfigurowania parametrów audytu dla usługi katalogowej umożliwiających między innymi: a) Śledzenie zmian obiektów usługi katalogowej z dostępem do informacji o dotychczasowej wartości b) Śledzenie zmian dotyczących tworzenia, usuwania obiektów Zamawiający wymaga skonfigurowania jednej stacji zarządzającej. Zarządzanie środowiskiem będzie się odbywać z poziomu stacji zarządzających (usługa katalogowa, wszystkie możliwe do zarządzania z poziomu stacji zarządzającej komponenty serwerów).
Konfiguracja polityki haseł oraz polityki blokowania kont	Konfiguracja globalnej polityki haseł dla domeny: a) Hasło musi zawierać minimum 8 znaków b) Maksymalny czas ważności hasła: do ustalenia z Zamawiającym c) Minimalny czas, po którym możliwa jest zmiana hasła: do ustalenia z Zamawiającym d) Hasło musi spełniać zasady złożoności Konfiguracja polityki haseł dla kadry zarządzającej: a) Hasło musi zawierać minimum 10 znaków b) Maksymalny czas ważności hasła: 30 dni c) Minimalny czas, po którym możliwa jest zmiana hasła: 30 dni d) Hasło musi spełniać zasady złożoności Po 3 nieudanych próbach uwierzytelniania konto powinno być blokowane na 30 minut. Automatyczne anulowanie blokady ma następować po 480 minutach. Szczegółowe dane zostaną przekazane na etapie konfiguracji.
Skonfigurowanie udostępniania zasobów sieciowych	Zamawiający wymaga uruchomienia oraz skonfigurowania macierzy o której mowa w punkcie 7 w taki sposób aby zostały spełnione poniższe założenia:

	3. Serwer plików musi być skonfigurowany w taki sposób, aby ograniczać ekspozycję danych dla użytkowników oraz grup, które nie mają do nich dostępu. 4. Na serwerze plików muszą być skonfigurowana przydziały dyskowe dla użytkowników i grup. Przydziały dyskowe zostaną określone przez Zamawiającego. 5. Zamawiający wymaga skonfigurowania parametrów audytu dla serwera plików umożliwiających między innymi: a) Określenie daty, czasu, nazwy użytkownika, który usunął / próbował usunąć plik/folder b) Określenie daty, czasu, nazwy użytkownika, który zapisał / próbował zapisać plik/folder c) Określenia daty, czasu, nazwy użytkownika, który próbował uzyskać nieuprawniony dostęp do zasobów, do których nie ma uprawnień. d) oraz określone przez Zamawiającego drukarki sieciowe. Zamawiający wymaga skonfigurowanie mapowania dysków sieciowych za pomocą zasad grup na dwa sposoby wykorzystaniem skryptów logowania lub z wykorzystaniem mechanizmów zaimplementowanych w systemach Microsoft Windows Vista i nowszych.
Uruchomienie oprogramowania do wykonywania kopii zapasowych środowiska wirtualnego	Instalacja oraz uruchomienie dostarczonego środowiska wykonywania kopii zapasowych ma zostać wykonana przy użyciu Serwera backupowego typ 1 określonego w punkcie 7 oraz oprogramowania do realizacji kopii zapasowych określonego w punkcie 12. Zamawiający wymaga aktywacji wymaganych licencji oraz konfiguracji zadań wykonywania kopii zapasowych wirtualnych maszyn według poniższych wymagań: 1. kopie wirtualnych maszyn muszą być wykonywane przy użyciu mechanizmów oferowanych przez dostarczone środowisko wirtualizujące; 2. kopie wirtualnych maszyn muszą być wykonywane na dedykowany zasób dyskowy; 3. kopie maszyn wirtualnych muszą być replikowane na wskazany przez Zamawiającego zasób dyskowy; 4. kopie wirtualnych maszyn muszą być wykonywane automatycznie wg zadanego harmonogramu; 5. kopie zapasowe muszą (jeżeli jest taka funkcjonalność) być wykonywane z zastosowaniem mechanizmów deduplikacji danych w celu zapewnienia inteligentnego zarządzania przestrzenią dyskową;

	Musi istnieć możliwość odtworzenia: 1. całej wirtualnej maszyny; 2. dysku wirtualnej maszyny; 3. pojedynczych plików wirtualnej maszyny (zamontowanie pliku z kopią zapasową w systemie operacyjnym gościa); Oprogramowanie musi umożliwiać: 1. replikację maszyn wirtualnych w oparciu o obrazy; 2. syntetyczną pełną kopię zapasową - tworzenie kopii zapasowych forever-incremental; 3. tworzenie harmonogramów kopii zapasowych bezpośrednio z UI; 4. weryfikację kopii zapasowej pod kątem infekcji i złośliwego oprogramowania przed przywróceniem do środowiska produkcyjnego; 5. konfigurację powiadomień o wykonaniu kopii zapasowej (e-mail). Zadaniem Wykonawcy będzie: 1. Uruchomienie testowych zadań backupu. 2. Weryfikacja poprawności wykonania kopii zapasowej / weryfikacja działania powiadomień email. 3. Uruchomienie testowych zadań odtworzenia danych.
Dołączenie stacji roboczych do domeny	Zamawiający wymaga dołączenia wszystkich dostarczonych oraz istniejących, kwalifikujących się stacji roboczych do domeny. W procesie dołączania stacji roboczych do domeny konieczne jest przeprowadzenie migracji profili użytkowników mająca na celu zachowanie specyficznych ustawień lokalnych kont użytkowników (między innymi zachowanie ustawień aplikacji oraz poczty elektronicznej). Po zalogowaniu się użytkownika na kont o domenowe użytkownik nie powinien zauważyć znaczących różnic w wyglądzie profilu (zachowane tapety oraz ustawienia pulpitu, dotychczas działające aplikacje powinny działać jak dotychczas bez potrzeby ponownej konfiguracji).
Wykonania prac instalacyjno-wdrożeniowych. Oddanie systemu do eksploatacji.	Wszystkie wymienione prace wdrożeniowe muszą zostać wykonane wspólnie z przedstawicielem Zamawiającego. Powyższe czynności należy wykonać w okresie realizacji Zamówienia po wcześniejszym uzgodnieniu harmonogramu wdrożenia z Zamawiającym.
Wdrożenie oprogramowania specjalistycznego	Zamawiający wymaga od wykonawcy, aby po zrealizowaniu dostawy komputerów przeprowadził wdrożenie i konfigurację oprogramowania specjalistycznego o którym mowa w punkcie 14.
Szkolenie dla administratora	Wykonawca w okresie wdrożenia przeprowadzi w siedzibie Zamawiającego szkolenia dla Administratora systemu, łącznie w wymiarze 18 godzin szkolenia (3 dni robocze). Szkoleniem zostaną objęte osoby

	wskazane przez Zamawiającego z zakresie dostarczonego rozwiązania teleinformatycznego, co najmniej w zakresie: ▪ Dostarczonego sprzętu (obsługi dostarczonych serwerów). ▪ Dostarczonego oprogramowania (systemu operacyjnego, systemu wirtualizacyjnego). ▪ Obsługi dostarczonego systemu backupu, archiwizacji danych oraz wykonywania kopii zapasowych. ▪ Zarządzania systemem firewall oraz przełącznikami sieciowymi. ▪ Obsługi oprogramowania specjalistycznego o którym mowa w punkcie 14 dla administratora (wymagana co najmniej 1 sesja - 2 godzinna). Celem szkolenia administratora będzie zapoznanie się z systemem informatycznym, poznanie poszczególnych funkcji i modułów oraz nauka jego obsługi w praktyce. Na etapie wdrożenia strony ustalą szczegółowy porządek i podział szkoleń z uwzględnieniem wymagań zawartych w niniejszym rozdziale, które przyjęte zostaną w planie szkoleń. Wykonawca zobowiązany jest do przeprowadzenia szkoleń w formie instruktażu stanowiskowego dla personelu w podziale na role w Systemie.
Opracowanie dokumentacji powykonawczej	Zamawiający wymaga opracowania szczegółowej dokumentacji technicznej użytkownika (w formie papierowej i elektronicznej)

14. ZAKUP SPECJALISTYCZNEGO OPROGRAMOWANIA

MINIMALNE WYMAGANIA FUNKCJONALNE, TECHNICZNE, UŻYTKOWE, JAKOŚCIOWE
Wymagania ogólne 1. Dostarczone licencje na oprogramowanie muszą być bezterminowe. 2. Dostarczone licencje na oprogramowanie muszą być dostarczone z 12 miesięcznym supportem producenta, liczonym od daty zakończenia wdrożenia, w okresie realizacji projektu, lecz nie dłużej niż do 30.09.2023 r. 3. W ramach supportu wymagany jest dostęp do nowych wersji systemu oraz wsparcia technicznego producenta. 4. Dostarczone licencje na oprogramowanie muszą objąć co najmniej 42 stanowiska komputerowych z systemem klasy Microsoft Windows, Licencje nie mogą mieć ograniczeń ilościowych dotyczących liczby obsługiwanych innych zasobów (np. drukarki, skanery, monitory itp). Ponadto musi posiadać co najmniej 1 licencję dostępową do konsoli zarządzającej. 5. W przypadku wątpliwości zamawiający zastrzega sobie prawo (w przeciągu do 7 dni od terminu otwarcia ofert) do wezwania wykonawcy do prezentacji zaoferowanego rozwiązania

celem weryfikacji zgodności z wymaganiami stawianymi przez zamawiającego w niniejszym postępowaniu.

Wymagania ogólne dla systemu zarządzania

1. Oprogramowanie musi posiadać polski oraz angielski interfejs językowy.
2. Oprogramowanie musi posiadać architekturę trójwarstwową składającą się z Bazy Danych, Serwera Aplikacji, Agenta/Konsoli zarządzającej.
3. Oprogramowanie musi umożliwiać obsługę dedykowanych kluczy szyfrujących podczas komunikacji pomiędzy agentami, serwerem aplikacji i konsolą zarządzającą.
4. Odczyt informacji dotyczących parametrów sprzętowych komputera musi odbywać się za pośrednictwem agenta systemu instalowanego na komputerach użytkowników.
5. Oprogramowanie musi umożliwiać wybór instalacji agenta w trybie standardowym oraz bezpiecznym tj. braku wkompilowanych funkcji takich jak zdalne zarządzanie, transfer plików, zdalny pulpit.
6. Oprogramowanie musi posiadać procedurę uwierzytelnienia i autoryzacji kont operatorów w konsoli zarządzającej poprzez fizyczne zabezpieczenie sprzętowe (lokalne lub sieciowe) wraz z hasłem, który umożliwia jednoczesną prace wielu administratorom. Logowanie użytkowników konsoli zarządzającej musi umożliwiać integrację z kontami Active Directory. Wymagane zabezpieczenie sprzętowe musi posiadać mechanizm szyfrowania danych AES w obrębie przechowywania danych wrażliwych.
7. Oprogramowanie musi posiadać moduł zarządzania uprawnieniami do poszczególnych funkcjonalności systemu dla operatorów konsoli zarządzającej zgodny z modelem RBAC (Role Based Access Control).
8. Oprogramowanie musi umożliwiać nadawanie oraz odbieranie uprawnień w czasie rzeczywistym (brak konieczności przelogowania użytkownika konsoli systemu).
9. Oprogramowanie musi umożliwiać blokadę wybranych uprawnień konkretnego użytkownika niezależnie od uprawnień wynikających z przypisanych ról.
10. Oprogramowanie musi współpracować z serwerem MSSQL Server 2008R2-2019
11. Oprogramowanie, w zakresie wszystkich warstw, nie może wymagać do prawidłowej pracy komponentów Java.
12. Oprogramowanie serwera aplikacji musi posiadać funkcjonalność centralnego wysyłania wybranych powiadomień mailowych .
13. Oprogramowanie musi posiadać moduł zarządzania uprawnieniami do danych w zakresie przypisywania wybranych jednostek organizacyjnych, Jednostek lokalizacyjnych oraz typów zasobów do poszczególnych użytkowników konsoli. Wszelkie raporty, zestawienia oraz funkcje obejmują wtedy tylko w/w przypisane obiekty.
14. Oprogramowanie musi być podpisane cyfrowo przez Producenta ważnym certyfikatem, z prawidłową ścieżką certyfikacji, w której główny urząd certyfikacji (Root CA) jest uczestnikiem programu certyfikatów głównych systemu Windows. Podpis cyfrowy dotyczy składników Producenta systemu w zakresie plików wykonywalnych (*.exe), plików bibliotek współdzielonych (*.dll), plików sterowników (*.sys) oraz pakietów instalacyjnych oprogramowania (*.msi).

15. Oprogramowanie agentów musi posiadać obsługę sesji terminalowych Windows.
16. Oprogramowanie musi zapewniać dowolną konfigurację pracy wszystkich agentów, jednostek organizacyjnych, pojedynczego agenta, poprzez dziedziczenie definiowanych przez administratora parametrów. Zmiany konfiguracji agentów następują w trybie natychmiastowym (online).
17. Oprogramowanie musi posiadać raport przedstawiający różnice w konfiguracji poszczególnych agentów w stosunku do konfiguracji globalnej.
18. Oprogramowanie musi posiadać mechanizm logowania zmian w konfiguracji agentów przez użytkowników konsoli (data, czas, login, poprzednia i nowa wartość).
19. Oprogramowanie musi posiadać mechanizm analizy czasu pracy komputera, informujący użytkownika (alert oraz wymuszone działanie – restart) o przekroczeniu zadanego czasu pracy bez restartu systemu operacyjnego.
20. Oprogramowanie musi zapewniać automatyczny import drzewiastej struktury organizacyjnej zamawiającego (bez ograniczeń ilości zagnieżdżeń z kontenera Active Directory/OpenLDAP), kont użytkowników i komputerów z zachowaniem ich oryginalnego położenia wg. OU.
21. Oprogramowanie musi zapewniać w obrębie synchronizacji z Active Directory/OpenLDAP tworzenie listy filtrów zawężających węzły danych wraz z możliwością wskazania docelowej gałęzi struktury organizacyjnej lub lokalizacyjnej Zamawiającego.
22. Oprogramowanie musi posiadać kreator powiązań (mapowanie atrybutów) dowolnych atrybutów obiektów z usługi katalogowej do wskazanych atrybutów zasobów systemowych.
23. Oprogramowanie musi umożliwiać współpracę z nieograniczoną ilością kontrolerów domen z zachowaniem podległej struktury drzewiastej.
24. Oprogramowanie musi umożliwiać automatyczny import informacji dotyczących przynależności użytkowników oraz stanowisk komputerowych do grup struktury katalogowej.
25. Oprogramowanie musi posiadać raport przedstawiający informacje nt. grup struktury katalogowej wraz przynależącymi do nich użytkownikami.
26. Oprogramowanie musi umożliwiać tworzenie dynamicznych grup stanowisk w oparciu o kreator zawierający filtry (AND, OR) w zakresie min. wersja OS, nazwa oraz wersja wybranej aplikacji, RAM, CPU, HDD, jednostka organizacyjna, jednostka lokalizacyjna, architektura (x32, x64), zainstalowane oprogramowanie, wersja oprogramowania, lista usług systemowych, producent oraz model komputera, poziom uprawnień, predefiniowane atrybuty komputera.
27. Oprogramowanie musi umożliwiać prezentację widoku zarządzanych stanowisk komputerowych w postaci listy stanowisk, drzewiastej struktury wg jednostek organizacyjnych, jednostek lokalizacyjnych, struktury Active Directory, struktury sieciowej (pule IP) oraz grup dynamicznych.
28. Oprogramowanie musi umożliwiać dynamiczne zawężanie wyników wyszukiwania ww. widoków na podstawie prezentowanych w nich atrybutów.
29. Oprogramowanie musi umożliwiać graficzną prezentację aktualnego stanu aktywności agenta (online/offline) z dokładnością do 1 minuty.
30. Oprogramowanie musi umożliwiać zapisywanie w bazie danych informacji o uruchomieniu i wyłączeniu komputera oraz zalogowaniu i wylogowaniu użytkownika

Inwentaryzacja konfiguracji komputerów

1. Oprogramowanie musi umożliwiać wydruk kartoteki sprzętowej stanowiska komputerowego.
2. Oprogramowanie musi umożliwiać samodzielną edycję wyglądu kartoteki sprzętowej, protokołów przekazania oraz zwrotu zasobów za pomocą graficznego kreatora wyglądu.
3. Oprogramowanie musi umożliwiać zapisywanie edytowanych szablonów (min. kartoteka sprzętowa, protokoły przekazania/zwrotu zasobów) w kontekście zalogowanego operatora konsoli zarządzającej.
4. Oprogramowanie musi umożliwiać projektowanie, generowanie oraz wydruk etykiet inwentaryzacyjnych w zakresie: model, nr inwentaryzacyjny, data zakupu, jednostka, wraz z obsługą kodów kreskowych w standardzie EAN128 oraz PDF417
5. Oprogramowanie musi umożliwiać okresową automatyczną inwentaryzację parametrów sprzętowych stanowiska: HDD, RAM, CPU, karta sieciowa, system operacyjny, karta graficzna itp.
6. Oprogramowanie Agenta musi umożliwiać audyt off-line, poprzez uruchomienie skanera (z GUI) bez konieczności instalacji, oraz zapis wyników do pliku w postaci zaszyfrowanej.
7. Oprogramowanie musi umożliwiać analizę sprzętową:
    - płyty głównej w zakresie model, producent, nr seryjny,
    - CPU w zakresie nazwy, modelu, producenta, częstotliwości,
    - HDD w zakresie numeru seryjnego dysku, numeru seryjnego partycji, rozmiaru pamięci,
    - RAM w zakresie wielkości pamięci,
    - karty sieciowej w zakresie model, adres IP, adres MAC,
    - karty graficznej w zakresie model.
8. Oprogramowanie musi umożliwiać odczyt informacji dotyczących systemu operacyjnego w zakresie nazwy, wersji, daty instalacji, zainstalowanych poprawek, dostępnych kluczy licencyjnych, produkt ID.
9. Oprogramowanie musi umożliwiać odczyt informacji sieciowych w zakresie adresu IO, adresu MAC, nazwy sieciowej.
10. Oprogramowanie musi umożliwiać odczyt informacji sprzętowych z BIOS w zakresie nazwy BIOS, daty, producenta.
11. Oprogramowanie musi umożliwiać przegląd historii zmian parametrów sprzętowych komputerowych.
12. Oprogramowanie musi umożliwiać globalny przegląd stanowisk komputerowych pod względem parametrów sprzętowo-systemowych.
13. Oprogramowanie musi zawierać raport stanowisk komputerowych posiadających co najmniej jedno konto z uprawnieniami administratora.
14. Oprogramowanie musi umożliwiać okresowe próbkowanie obciążenia procesora oraz zajętości pamięci RAM z możliwością zapisu odczytanych wyników do bazy w celu późniejszej analizy (historia obciążenia komputera).

Inwentaryzacja oprogramowania

1. Oprogramowanie musi umożliwiać automatyczną inwentaryzację zainstalowanego na komputerach oprogramowania.
2. Oprogramowanie musi umożliwiać globalny przegląd wszystkich programów zainstalowanych na komputerach.
3. Oprogramowanie musi umożliwiać tworzenie zestawień zainstalowanych typów programów (freeware, shareware itp.).
4. Oprogramowanie musi umożliwiać tworzenie wykazów z zainstalowanym, dowolnie wybranym programem.
5. Oprogramowanie musi umożliwiać tworzenie zestawień zainstalowanych systemów operacyjnych na komputerach.
6. Oprogramowanie musi umożliwiać tworzenie wykazów stanowisk z brakiem zainstalowanego, dowolnie wybranego, programu.
7. Oprogramowanie musi posiadać wbudowany mechanizm umożliwiający, poprzez GUI konsoli, zdalną grupową dezinstalację oprogramowania np. pakietów MS Office.
8. Oprogramowanie musi umożliwiać oznaczanie kolorem aplikacji zabronionych oraz zgodnych ze standardem wraz z możliwością raportowania wg w/w klasyfikacji.
9. Oprogramowanie musi umożliwiać okresowe skanowanie aktualnie uruchomionych procesów systemowych wraz z historią występowania procesu podczas wcześniejszych skanów.
10. Oprogramowanie musi umożliwiać zablokowanie na stacji roboczej wybranych procesów celem uniemożliwienia ich uruchomienia przez użytkownika.

Oprogramowanie musi posiadać globalne zestawienie pozwalające na zdalne usunięcie nielegalnych danych np. plików AVI, MP3, MP4 bez konieczności fizycznej obecności użytkownika przy stacji.

Zarządzanie licencjami, audyt oprogramowania

1. Oprogramowanie musi posiadać wbudowaną bazę sygnatur aplikacji (produktów) wraz z możliwością automatycznej aktualizacji wzorców ze strony Producenta oprogramowania
2. Oprogramowanie musi umożliwiać zdefiniowanie własnych sygnatur aplikacji (produktów) wykorzystywanych w procesie automatycznego audytu licencji (rozliczenie ilościowe).
3. Oprogramowanie musi umożliwiać wykonanie audytu licencji tj. systemowego porównania zidentyfikowanego na stanowiskach komputerowych oprogramowania (produktów) z zakupionymi licencjami wprowadzonymi do systemu jako odpowiednie obiekty. Mechanizm audytu musi umożliwiać rozliczenie licencji z wykorzystaniem mechanizmów downgrade, upgrade.
4. Oprogramowanie musi umożliwiać zapis historii wykonywanych audytów licencji.

Oprogramowanie musi umożliwiać tworzenie bazy licencji systemowo/programowych i przypisywanie ich do stanowisk komputerowych oraz użytkowników.

Zarządzanie zasobami oraz użytkownikami

1. Oprogramowanie musi umożliwiać klonowanie wybranych typów zasobów.
2. Oprogramowanie musi umożliwiać tworzenie własnych szablonów widoków zasobów z określeniem analizowanych typów zasobów, widocznych atrybutów oraz informacji nt. powiązań pomiędzy zasobami.

3. Oprogramowanie musi umożliwiać tworzenie własnych atrybutów o typach co najmniej: tekst, liczba, bit, data, wartość słownikowa dla wybranego typu zasobu.
4. Oprogramowanie musi umożliwiać zapis oraz przegląd historii zmian dowolnego atrybutu zasobu w zakresie: operator, data, czas, poprzednia oraz nowa wartość.
5. Oprogramowanie musi umożliwiać zdefiniowanie dowolnych relacji pomiędzy zasobami (np. powiązania stanowiska z pracownikiem, licencją, innym zasobem) wraz z zapisem historii relacji zasobów.
6. Oprogramowanie musi umożliwiać zdefiniowanie dodatkowych atrybutów dla wybranych relacji pomiędzy zasobami w zakresie zgodnym z atrybutami typów zasobów.
7. Oprogramowanie musi umożliwiać przypisywanie do każdego z zarządzanych w systemie zasobów dokumentów typu: faktura zakupu, gwarancja, umowa serwisowa. Bazą dokumentów musi być centralne repozytorium umożliwiające powiazania dokumentów z zasobami w relacji 1:N wraz z podglądem przypisanych zasobów oraz wydrukiem.
8. Oprogramowanie musi umożliwiać zdefiniowanie dowolnego zasobu inwentaryzacyjnego (np. telefon, drukarka, nawigacja) wraz z kreatorem widocznych/wymaganych atrybutów edycyjnych.
9. Oprogramowanie musi posiadać dedykowaną (zintegrowaną z systemem) aplikację na platformę Android umożliwiającą spis z natury zinwentaryzowanych zasobów.
10. Oprogramowanie musi umożliwiać import danych z zewnętrznego pliku CSV zawierającego informacje inwentaryzacyjne z nowo zakupionych urządzeń w zakresie: numer faktury, numer seryjny, model, nazwa, data zakupu.
11. Oprogramowanie musi umożliwiać zaprojektowanie własnego schematu importu danych z zewnętrznego pliku CSV.
12. Oprogramowanie musi umożliwiać automatyczne tworzenie relacji pracownik-komputer na podstawie atrybutów obiektu w usłudze katalogowej.

Zdalny pulpiy, zdalne zarządzanie komputerem

1. Oprogramowanie musi umożliwiać interakcję administratora z użytkownikiem, polegającą na podłączeniu do stanowiska (przejęcie pulpitu) administratora bez konieczności uprzedniego wylogowania użytkownika. Funkcjonalność zdalnego pulpitu nie może wymagać instalacji aplikacji firm trzecich, wymagane jest obsłużenie przejęcia zdalnego pulpitu przez mechanizm wbudowany w agencie (ten sam proces systemowy).
2. Oprogramowanie musi umożliwiać wybór monitora, którego ekran ma zostać przejęty podczas połączenia zdalnego. Podczas aktywnego połączenia zdalnego, użytkownik jest informowany o trwaniu sesji zdalnej poprzez wyświetlanie na aktywnym monitorze kontrastowego obramowania ekranu.
3. Oprogramowanie musi umożliwiać zdalne zarządzanie (bez użycia RDP/VNC itp.) lokalnymi kontami użytkowników w zakresie (tworzenie, usuwanie, edycja, zmiana hasła oraz typ konta).
4. Oprogramowanie musi umożliwiać wysyłanie polecenia Wake-on LAN.
5. Oprogramowanie musi umożliwiać zdalną dwukierunkową linię poleceń.

6. Oprogramowanie musi umożliwiać przesyłanie plików/katalogów od zdalnego użytkownika do administratora i/lub od administratora do zdalnego użytkownika bez względu na lokalizację sieciową komputera (LAN, WAN, Internet).
7. Oprogramowanie musi umożliwiać konfigurację przez administratora parametrów połączenia z użytkownikiem w zakresie: ilość kolorów, ilość klatek/sekundę, skalowanie okna użytkownika, jeżeli jest ono większe niż rozdzielczość stacji administratora.
8. Oprogramowanie musi umożliwiać wybór aktywnych sesji terminalowych, do których chcemy się podłączyć.
9. Oprogramowanie musi umożliwiać zbiorczy podgląd zdalnych pulpitów stacji.
10. Oprogramowanie musi posiadać zarządzanie technologią iAMT, vPro w zakresie uwzględniającym min.: Serial Over Lan (SOL), IDE Redirection (IDER), Hardware KVM, Assets.
11. Oprogramowanie musi zapewniać zdalną konfigurację technologii iAMT w trybie Client Control Configuration Mode.
12. Oprogramowanie musi umożliwiać zarządzanie stacjami komputerowymi poza siecią LAN/WAN, wymagane jest tylko dowolne połączenie internetowe.
13. Oprogramowanie musi umożliwiać zdalne wykonywanie zapytań WQL.
14. Oprogramowanie musi umożliwiać zdalny odczyt oraz modyfikację rejestru Windows.
15. Oprogramowanie musi umożliwiać pełne wykorzystanie funkcji zawartych w sekcji zdalne zarządzanie dla stacji posiadających dowolne połączenie do sieci INTERNET bez konieczności zestawiania połączenia VPN.
16. Oprogramowanie musi umożliwiać przejęcie pulpitu zdalnego z poziomu konsoli zarządzającej znajdującej się poza siecią LAN organizacji poprzez połącznie konsoli ze wskazanym serwerem aplikacji.
17. Oprogramowanie musi umożliwiać prowadzenie w czasie rzeczywistym dwukierunkowej komunikacji tekstowej (chat) pomiędzy użytkownikiem a administratorem.

Automatyzacja

1. Oprogramowanie musi umożliwiać zdalną instalację pakietów *.msi, plików *.cmd, *.bat, *.reg, *.ps1 poprzez utworzenie zadań dystrybucji aplikacji oraz wskazanie docelowych komputerów lub grup komputerów za pomocą dedykowanego GUI użytkownika. Zadanie dystrybucji musi umożliwiać określenie okresu aktywności, godziny rozpoczęcia oraz przedstawiać status instalacji na wybranych stanowiskach.
2. Oprogramowanie musi umożliwiać tworzenie zadań dystrybucji polegające na jednorazowym uruchomieniu wybranego szablonu akcji na wybranych stanowiskach komputerowych.
3. Oprogramowanie musi umożliwiać tworzenie polis uruchamianych cyklicznie na wybranych stanowiskach komputerowych wg aktualnej przynależności do struktury organizacyjnej, lokalizacyjnej lub wybranych grup dynamicznych.
4. Oprogramowanie musi umożliwiać tworzenie dystrybucji zadań oraz polis dla wybranych stanowisk komputerowych poprzez interaktywny kreator (krok po kroku). Wybór odbiorców musi uwzględniać listę stanowisk, strukturę organizacyjną, strukturę lokalizacyjną oraz dynamiczne grupy stanowisk.

5. Oprogramowanie musi umożliwiać globalną dystrybucję plików oraz folderów do wskazanych lokalizacji do wybranych stanowisk komputerowych wg przynależności do struktury organizacyjnej, lokalizacyjnej lub grupy dynamicznej wraz z automatycznym (polisa) odtworzeniem brakujących danych w przypadku wykrycia niespójności.
6. Oprogramowanie musi umożliwiać szyfrowanie plików źródłowych dla zadań instalacji.
7. Oprogramowanie musi umożliwiać globalny przegląd postępu wykonania wybranych zadań oraz polis wraz z odczytem standardowego wyjścia (stdout) oraz standardowego wyjścia błędów (stderr).
8. Oprogramowanie musi umożliwiać tworzenie własnych szablonów akcji zawierających zdefiniowaną listę akcji pozwalających na warunkowe uruchamianie akcji zależnych (oczekiwanie na zakończenie akcji, praca w tle).
9. Oprogramowanie musi umożliwiać konfigurację typów akcji co najmniej w zakresie: dystrybucja i uruchomienie plików wsadowego BAT, dystrybucja plików rejestru REG, dystrybucja i instalacja pakietu MSI, dystrybucja i instalacja poprawki MSP, dystrybucja i uruchomienie aplikacji EXE, dystrybucja i uruchomienie skryptu PowerShell, dystrybucja plików i folderów, uruchomienie/wyłączenie/restart usługi systemowej, zakończenie procesu systemowego, wywołanie polecenia CMD.
10. Oprogramowanie musi umożliwiać konfigurowanie dedykowanych parametrów dla każdej z ww. akcji.
11. Oprogramowanie musi umożliwiać uruchomienie na prawach administracyjnych pliku instalacyjnego EXE (z GUI) w sesji użytkownika z ograniczonymi uprawnieniami do instalacji aplikacji. Proces instalacji jest manualnie kontynuowany przez użytkownika.
12. Oprogramowanie musi umożliwiać ograniczenie zakresu działania zadania, polisy oraz zawężenie wszelkich raportów systemowych do stanowisk spełniających kryteria wybranej dynamicznej grupy stanowisk.
13. Oprogramowanie musi umożliwiać optymalizację dystrybucji zadań oraz plików na komputery, pobierając brakujące fragmenty plików od agentów z tej samej podsieci (mechanizm peer-to-peer).
14. Oprogramowanie w zakresie automatyzacji musi realizować m.in. następujące przypadki użycia z wykorzystaniem mechanizmu grup dynamicznych dla zadań oraz polis:
    a) Automatyczną instalacji aplikacji na komputerach spełniających warunki: stanowiska z Windows 10 z pamięcią RAM>4GB i zainstalowaną wybraną aplikacją w wersji mniejszej (np. 7.0)
    b) Automatyczne odinstalowanie aplikacji na komputerach spełniających warunki: stanowiska z Windows 7 gdzie producentem komputera jest np. Dell i zainstalowaną wybraną aplikacją w wersji większej niż (np. 8.0)
    c) Dystrybucję plików oraz folderów (ze wskazaną zawartością np. dokumenty, skróty do aplikacji) na pulpity stanowisk komputerowych spełniających warunki: stanowiska z Windows 10 z brakiem zainstalowanej wybranej aplikacji oraz nie posiadające konta użytkownika z prawami administracyjnymi

d) Uruchomienia wybranego skryptu PowerShell dla komputerów spełniających warunki: stanowiska z Windows 10 w architekturze 32 bitowej, zainstalowaną aplikacją X w wersji większej niż (np. 6.0) i brakiem zainstalowanej aplikacji Y.
e) Uruchomienia wybranych szablonów akcji w przypadku wykrycia zmiany jednostki organizacyjnej stanowiska komputerowego.

15. W przypadku wcześniej zdefiniowanych polis wymagane jest, aby zostały one automatycznie uruchomione dla nowych stanowisk komputerowych po spełnieniu warunków przynależności do określonych grup dynamicznych

Backup danych użytkownika

1. Oprogramowanie musi umożliwiać tworzenie dowolnej ilości automatycznych zadań w zakresie archiwizacji danych – globalnie z poziomu głównej konsoli zarządzającej.
2. Oprogramowanie musi umożliwiać globalną zmianę parametrów zadań archiwizacji (ilość archiwów, kompresja, okres, zakres).
3. Oprogramowanie musi umożliwiać definiowanie rozszerzeń plików, które mają być pomijane podczas procesu archiwizacji oraz rozszerzeń plików np. *.doc, które mają być archiwizowane.
4. Oprogramowanie Agenta musi umożliwiać kopię całościową danych oraz przesyłanie plików z archiwizacji na wskazany serwer FTP.
5. Mechanizm archiwizacji danych musi być realizowany przez Agenta systemu bez udziału zdalnych sesji (typu zdalny pulpit, wywoływanie skryptów)
6. Oprogramowanie musi umożliwiać definiowanie cyklu archiwizacji.
7. Oprogramowanie musi umożliwiać automatyczne usuwanie starszych plików kopii całościowej, definiowanie globalnego zadania archiwizacji

Zarządzanie urządzeniami

1. Oprogramowanie musi umożliwiać zapisywanie w bazie danych informacji o kopiowaniu z/do urządzeń zewnętrznych typu: Pendrive USB, dysk zewnętrzny.
2. Oprogramowanie musi posiadać raport w zakresie rejestracji informacji na temat użytkownika, który kopiował i/lub uruchamiał napęd, kiedy miało miejsce zdarzenie i jakie dokumenty zostały skopiowane.
3. Oprogramowanie musi umożliwiać blokadę oraz autoryzację wybranych urządzeń USB w obrębie klasy USBStorage.
4. Oprogramowanie musi umożliwiać włączenie trybu ReadOnly dla klasy USBStorage
5. Oprogramowanie musi umożliwiać całkowitą blokadę klasy FDD/CD/DVD

Zarządzanie zgłoszeniami

1. Oprogramowanie w części HelpDesk musi być oparte na zasadach ITIL w szczególności:
   a) Zarządzanie problemem
   b) Zarządzanie incydentem
   c) Obsługa procesów poprzez WorkFlow (wnioski o usługi, uprawnienia, zakupy)
   d) Zarządzanie umowami serwisowymi

e) Definicje poziomów SLA (reakcja, naprawa, reklamacja)

2. Oprogramowanie musi umożliwiać zgłaszania przez użytkowników z poziomu przeglądarki WWW (dedykowany portal) awarii sprzętu, usług, oprogramowania i innych typów awarii zdefiniowanych przez administratora.
3. Portal ServiceDesk musi mieć możliwość obsługi przez wiodące przeglądarki WWW na urządzeniach mobilnych poprzez responsywny interfejs użytkownika.
4. Portal ServiceDesk musi zostać dostarczony w technologii PHP w formie otwartych źródeł z możliwością samodzielnej edycji kodu.
5. Portal ServiceDesk musi umożliwiać wybór wersji językowej interfejsu (co najmniej polski i angielski).
6. Obsługa listy zgłoszeń serwisowych (incydentów i problemów) musi być realizowana przez portal ServiceDesk z zachowaniem nadanego poziomu uprawnień.
7. Oprogramowanie musi umożliwiać kontrolę obciążenia działu IT, optymalizację podziału pracy pomiędzy pracowników działu IT oraz przegląd awaryjności sprzętu.
8. Oprogramowanie musi umożliwiać uwierzytelnianie użytkowników wykorzystując bazę Active Directory poprzez protokół LDAP.
9. Oprogramowanie musi umożliwiać automatyczne autoryzowanie określonych stanowisk i użytkowników (z wykorzystaniem mechanizmy SSO), aby uniknąć każdorazowego uwierzytelniania przed korzystaniem z systemu zgłoszeń.
10. Oprogramowanie musi umożliwiać sortowanie listy zgłoszeń awarii, wg daty zgłoszenia, priorytetu, statusu.
11. Oprogramowanie musi umożliwiać filtrację zgłoszeń wg priorytetu oraz statusów zgłoszeń, stanowisk oraz inżynierów obsługujących zgłoszenia.
12. Oprogramowanie musi umożliwiać tworzenie dedykowanych list zgłoszeń z różnymi danymi, domyślnym filtrowaniem i sortowaniem.
13. Oprogramowanie musi umożliwiać określenie widoczności poszczególnych list zgłoszeń w zależności od zalogowanego użytkownika.
14. Oprogramowanie musi umożliwiać określenie widoczności zgłoszeń w zależności od kategorii i lokalizacji zgłoszeń przypisanych do zalogowanego użytkownika.
15. Oprogramowanie musi umożliwiać dostęp do zgłoszeń swoich podwładnych przez przełożonego.
16. Oprogramowanie musi umożliwiać edycję kilku zgłoszeń jednocześnie po wyborze z listy zgłoszeń.
17. Oprogramowanie musi umożliwiać dodawanie przez administratora nowych wpisów (komentarzy) w zgłoszeniu, jak i umożliwiać zmianę statusu sprawy. Użytkownik także ma możliwość dodawania nowych wpisów do zgłoszonego problemu wraz ze zmianą statusu.
18. Oprogramowanie musi umożliwiać tworzenie zadań w ramach konkretnego zgłoszenia z możliwością przekazania do realizacji przez innych użytkowników.
19. Oprogramowanie musi umożliwiać tworzenie globalnych zadań do realizacji przez zalogowanego użytkownika.
20. Oprogramowanie musi umożliwiać tworzenie szablonów zadań.

21. Oprogramowanie musi umożliwiać rejestrację czasu pracy poświęconego na realizację zgłoszenia przez opiekuna.
22. Oprogramowanie musi umożliwiać administratorowi ustalanie statusów i priorytetów z zaznaczeniem, które z nich może używać użytkownik zgłaszający problem.
23. Oprogramowanie musi umożliwiać przesyłanie użytkownikom powiadomień pocztą elektroniczną o nowych wpisach i zmianach w zgłoszeniu.
24. Oprogramowanie musi umożliwiać obsługę autoryzacji OAuth 2.0 w zakresie powiadomień mailowych oraz rejestracji zgłoszeń drogą mailową.
25. Oprogramowanie musi umożliwiać edycję szablonów powiadomień email.
26. Oprogramowanie musi umożliwiać tworzenie wielopoziomowych list kategorii zawierających nazwę i opis kategorii.
27. Oprogramowanie musi umożliwiać określenie widoczności poszczególnych kategorii w zależności od zalogowanego użytkownika.
28. Oprogramowanie musi umożliwiać określenie widoczności poszczególnych statusów i priorytetów w zależności od zalogowanego użytkownika.
29. Oprogramowanie musi umożliwiać tworzenie pól dodatkowych na formularzu rejestracji zgłoszenia.
30. Oprogramowanie musi umożliwiać określenie widoczności poszczególnych pól dodatkowych w zależności od zalogowanego użytkownika.
31. Zapisane przez administratora rozwiązania incydentów tworzą bazę wiedzy (powiązaną z kategoriami) Baza ta wyświetlana jest użytkownikom podczas przeglądania kategorii zgłoszeń. Rozwiązania w bazie wiedzy muszą posiadać znacznik określający czy są dostępne dla użytkowników, czy są wewnętrznymi uwagami działu IT. Panel www użytkownika musi zawierać wyszukiwarkę tematów wg słów kluczowych oraz wewnętrznej treści.
32. Oprogramowanie musi umożliwiać edycję bazy wiedzy z poziomu przeglądarki WWW wraz z możliwością formatowania tekstu (wraz z grafiką) oraz wstawiania załączników.
33. Oprogramowanie musi umożliwiać administratorowi wprowadzenie do systemu zgłoszenia użytkownika, który nie ma dostępu do PC (np. telefonicznie informuje, że zepsuł mu się komputer).
34. Oprogramowanie musi umożliwiać delegowanie zgłoszenia innemu administratorowi (technikowi), jak również przejęcie innego zgłoszenia (np. w przypadku nieplanowanej nieobecności pracownika).
35. Oprogramowanie musi umożliwiać obsługę tzw. Linii wsparcia poprzez samodzielne tworzenie nowych linii wraz z przypisywaniem do nich dowolnej ilości kont operatorów HelpDesk. Zgłoszenie serwisowe musi mieć możliwość przekazania do dowolnej linii wsparcia lub dedykowanego operatora HelpDesk. Linia wsparcia musi mieć możliwość przypisania powiązanych z nią kategorii zgłoszeń.
36. Oprogramowanie musi umożliwiać informowanie pracowników o planowanych działaniach, awariach za pomocą komunikatów wprowadzanych na stronę główną panelu zgłaszania usterki, bądź do poszczególnych kategorii.
37. Oprogramowanie musi umożliwiać określenie widoczności komunikatów o planowanych działaniach, awariach w zależności od zalogowanego użytkownika.

38. Oprogramowanie musi umożliwiać dostęp lub ograniczenie dostępu do ogłoszeń lub bazy wiedzy dla anonimowego użytkownika.
39. Oprogramowanie musi umożliwiać tworzenia baz umów serwisowych powiązanych z bazami firm serwisowych (dostawców sprzętu, oprogramowania, lokalnych serwisów). Możliwość powiązania każdej umowy z zakupionymi licencjami oprogramowania lub z zakupionym sprzętem.
40. Oprogramowanie w oparciu o bazę firm/umów serwisowych musi umożliwiać zapis przekazania zgłoszenia do serwisu zewnętrznego.
41. Oprogramowanie musi umożliwiać przesyłanie powiadomień do firm serwisowych powiązanych ze zgłoszeniem.
42. Oprogramowanie musi posiadać możliwość rejestracji w historii zgłoszenia (w komentarzach) korespondencji
43. mailowej między opiekunami zgłoszenia a firmami serwisowymi powiązanymi ze zgłoszeniem.
44. Oprogramowanie musi posiadać dedykowane panele WWW w zależności od aktywnie zalogowanego użytkownika końcowego (panel dla użytkownika tj. zgłaszanie incydentów, panel dla operatora serwisowego - obsługa zgłoszeń, panel dla managera HelpDesk – analiza graficzna oraz tabelaryczna pracy operatorów HelpDesk).
45. Oprogramowanie musi umożliwiać wyświetlenie w panelu WWW użytkownika informacji nt. powiązanych z użytkownikiem zasobów (przypisane stanowiska PC, przydzielone licencje aplikacji, wydane urządzenia).
46. Oprogramowanie musi umożliwiać wybranie zasobu w określonej kategorii powiązanego z użytkownikiem podczas rejestracji zgłoszenia.
47. Oprogramowanie musi umożliwiać tworzenie zgłoszeń cyklicznych z możliwością definiowania częstości występowania oraz typu okresu (codziennie, co tydzień, co miesiąc)
48. Oprogramowanie musi umożliwiać klonowanie zgłoszeń.
49. Oprogramowanie musi umożliwiać tworzenie reguł w celu automatyzacji obsługi zgłoszeń. Reguły muszą uruchamiać się w odpowiedzi na określone zdarzenia w systemie i wykonywać akcje w zależności od spełnionych warunków. W zakresie reguł ServiceDesk musi realizować m.in. następujące przypadki użycia:
    a) Zmiana statusu po przejęciu zgłoszenia przez opiekuna.
    b) Przejmowanie zadań po przejęciu zgłoszenia przez opiekuna.
    c) Dodawanie zadań w zgłoszeniu w zależności od parametrów zgłoszenia.
    d) Wznawianie zgłoszenia po odpowiedzi przez zgłaszającego użytkownika.
    e) Zamykanie zgłoszenia po upływie czasu bez odpowiedzi użytkownika.
    f) Zamykanie zgłoszenia po upływie czasu reklamacji.
    g) Dodawanie wpisów (komentarzy) w zgłoszeniu na podstawie szablonów.
    h) Zmiana parametrów zgłoszenia po znalezieniu wybranej frazy w treści komentarza.
    i) Walidacja zamkniętych zadań w zamykanym zgłoszeniu.
    j) Systemowe potwierdzanie realizacji zgłoszenia.
    k) Wysyłanie dodatkowych powiadomień cyklicznych ze zgłoszeniami, np. zgłoszenia wymagające reakcji, zgłoszenia do realizacji lub zgłoszenia wstrzymane/wznowione.

50. Oprogramowanie musi umożliwiać tworzenie szablonów komentarzy wykorzystywanych przez opiekunów zgłoszeń.
51. Oprogramowanie musi posiadać możliwość rejestracji zgłoszeń i komentarzy drogą mailową, zarówno przez zarejestrowanych użytkowników systemu jak i niezarejestrowanych użytkowników.
52. Oprogramowanie musi umożliwiać obsługę dowolnej ilości kont pocztowych do wysyłania powiadomień i generowania zgłoszeń/komentarzy przez email.
53. Oprogramowanie musi umożliwiać wyświetlenie w panelu WWW operatora HelpDesk informacji nt. aktywności zarejestrowanych stanowisk (on-line/off-line) oraz alertów dotyczących obciążenia CPU, RAM, HDD.
54. Oprogramowanie musi posiadać wbudowane raporty prezentujące m.in. realizację obsługi zgłoszeń w zakładanym SLA (statystyka miesięczna, kwartalna, roczna).

Monitoring sieci LAN

1. Oprogramowanie musi umożliwiać okresowe skanowanie sieci LAN (wg. zadanych kryteriów, na wybranych serwerach lokalnych) z wykorzystaniem protokołu SNMP, celem prezentacji aktywnych urządzeń IP w zakresie co najmniej komputery, drukarki, routery, smartphony
2. Oprogramowanie musi umożliwiać monitorowanie poprzez wykorzystanie protokołu SNMP stanu drukarek tj. poziomy tonerów, liczba wydrukowanych stron oraz informować błędach takich jak brak papieru, zacięcie papieru.
3. Oprogramowanie musi umożliwiać wizualizację ruchu sieciowego na poszczególnych portach urządzeń sieciowych wraz z wizualizacją w postaci mapy sieci dla wskazanego urządzenia typu switch, router.
4. Oprogramowanie musi umożliwiać z zdalną instalację agenta systemu z poziomu wykrytej struktury sieciowej z wykorzystaniem poświadczeń administracyjnych, w tym również stanowisk poza usługą katalogową.
5. Oprogramowanie musi umożliwiać monitorowanie stanu dowolnej usługi sieciowej TCP.
6. Oprogramowanie musi umożliwiać monitorowanie dowolnego licznika SNMP(v1/2/3) urządzenia.
7. Oprogramowanie musi umożliwiać monitorowanie stanu dowolnego urządzenia sieciowego poprzez odpytywanie typu PING.
8. Oprogramowanie musi umożliwiać tworzenie konfigurowalnych zdarzeń sieciowych powodujących wysyłanie komunikatów informacyjnych i/lub ostrzegawczych poprzez SMS i/lub Email.

System wewnętrznego komunikatora dla użytkowników

1. Oprogramowanie musi zawierać wewnętrzny komunikator pracujący w sieci LAN, integrujący się z usługą katalogową w zakresie kont użytkowników (dane osobowe, avatar), jednostek organizacyjnych.
2. Oprogramowanie w zakresie modułu komunikatora dla użytkowników musi współpracować z serwerem MSSQL Server 2008R2-2019 lub PostrgeSQL

3. Oprogramowanie komunikatora musi umożliwiać automatyczne logowanie użytkowników pochodzących z usługi katalogowej. 4. Oprogramowanie komunikatora musi umożliwiać konwersację grupową oraz prywatną pomiędzy użytkownikami 5. Oprogramowanie komunikatora musi umożliwiać wysyłanie wiadomości powitalnych; komunikatów grupowych z raportowaniem doręczenia oraz odczytania. 6. Oprogramowanie komunikatora musi umożliwiać generowanie raportów doręczenia/odczytania wiadomości wymagających potwierdzenia. 7. Oprogramowanie komunikatora musi umożliwiać określenie maksymalnego rozmiaru transferowanego pliku (przez administratora). 8. Oprogramowanie komunikatora musi umożliwiać wysyłanie powiadomień e-mail o utworzeniu/modyfikacji użytkowników, którzy nie pochodzą z usługi katalogowej. 9. Oprogramowanie komunikatora musi umożliwiać automatyczną aktualizację wg. zadanej konfiguracji danych synchronizowanych (ze szczególnym uwzględnieniem danych o użytkownikach, jednostkach organizacyjnych z usługi katalogowej). 10. Oprogramowanie komunikatora musi umożliwiać archiwizację starych rozmów między użytkownikami. 11. Oprogramowanie komunikatora musi umożliwiać administratorowi wyłączenie globalnie możliwości zamknięcia/wylogowanie/zapisywanie poświadczeń dla klientów końcowych. 12. Oprogramowanie komunikatora musi umożliwiać administratorowi bezpieczeństwa wgląd do rozmów pracowników, wyłączenie wybranych funkcjonalności dla klienta końcowego (np. transferu plików, konferencji audio-video). 13. Oprogramowanie komunikatora musi umożliwiać wymianę plików pomiędzy zalogowanymi użytkownikami 14. Oprogramowanie komunikatora musi umożliwiać nawiązanie sesji audio oraz wideo pomiędzy zalogowanymi użytkownikami wraz z obsługą konferencji grupowych

15. ROZBUDOWA ZABEZPIECZEŃ LOGICZNYCH (FIREWALL, IDS, IPS)

ATRYBUT	MINIMALNE WYMAGANIA FUNKCJONALNE, TECHNICZNE, UŻYTKOWE, JAKOŚCIOWE
Ilość	1 zestaw
Określenie oferowanej konfiguracji	Zamawiający wymaga określenia przez oferenta w formularzu ofertowym co najmniej następujących cech oferowanego rozwiązania: producent (marka), model (symbol), gwarancja, licencje, pakiety wsparcia
Wymagania ogólne	Dostarczony system bezpieczeństwa musi zapewniać wszystkie wymienione poniżej funkcje sieciowe i bezpieczeństwa niezależnie od dostawcy łącza. Dopuszcza się aby poszczególne elementy wchodzące w skład systemu bezpieczeństwa były zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub komercyjnych aplikacji instalowanych na platformach ogólnego przeznaczenia. W przypadku

	implementacji programowej dostawca musi zapewnić niezbędne platformy sprzętowe wraz z odpowiednio zabezpieczonym systemem operacyjnym. System realizujący funkcję Firewall musi dawać możliwość pracy w jednym z trzech trybów: Routera z funkcją NAT, transparentnym oraz monitorowania na porcie SPAN. W ramach dostarczonego systemu bezpieczeństwa musi być zapewniona możliwość budowy minimum 2 oddzielnych (fizycznych lub logicznych) instancji systemów w zakresie: Routingu, Firewall'a, IPSec VPN, Antywirus, IPS, Kontroli Aplikacji. Powinna istnieć możliwość dedykowania co najmniej 4 administratorów do poszczególnych instancji systemu. System musi wspierać IPv4 oraz IPv6 w zakresie: ▪ Firewall. ▪ Ochrony w warstwie aplikacji. ▪ Protokołów routingu dynamicznego.
Redundancja, monitoring i wykrywanie awarii	1. W przypadku systemu pełniącego funkcje: Firewall, IPSec, Kontrola Aplikacji oraz IPS - musi istnieć możliwość łączenia w klaster Active-Active lub Active-Passive. W obu trybach powinna istnieć funkcja synchronizacji sesji firewall. 2. Monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łączy sieciowych. 3. Monitoring stanu realizowanych połączeń VPN. 4. System musi umożliwiać agregację linków statyczną oraz w oparciu o protokół LACP. Powinna istnieć możliwość tworzenia interfejsów redundantnych.
Interfejsy, Zasilanie:	1. System realizujący funkcję Firewall musi dysponować minimum: ▪ 10 portami Gigabit Ethernet RJ-45. ▪ 2 gniazdami SFP 1 Gbps. 2. System Firewall musi posiadać wbudowany port konsoli szeregowej oraz gniazdo USB umożliwiające podłączenie modemu 3G/4G oraz instalacji oprogramowania z klucza USB. 3. W ramach systemu Firewall powinna być możliwość zdefiniowania co najmniej 200 interfejsów wirtualnych definiowanych jako VLAN'y w oparciu o standard 802.1Q. 4. System musi być wyposażony w zasilanie AC.
Parametry wydajnościowe	1. W zakresie Firewall'a obsługa nie mniej niż 1.4 mln. jednoczesnych połączeń oraz 45 tys. nowych połączeń na sekundę. 2. Przepustowość Stateful Firewall: nie mniej niż 10 Gbps dla pakietów 512 B. 3. Przepustowość Firewall z włączoną funkcją Kontroli Aplikacji: nie mniej niż 1.7 Gbps. 4. Wydajność szyfrowania IPSec VPN nie mniej niż 6 Gbps.

	5. Wydajność skanowania ruchu w celu ochrony przed atakami (zarówno client side jak i server side w ramach modułu IPS) dla ruchu Enterprise Traffic Mix - minimum 1.4 Gbps. 6. Wydajność skanowania ruchu typu Enterprise Mix z włączonymi funkcjami: IPS, Application Control, Antywirus - minimum 900 Mbps. 7. Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL dla ruchu http – minimum 700 Mbps.
Funkcje Systemu Bezpieczeństwa	W ramach dostarczonego systemu ochrony muszą być realizowane wszystkie poniższe funkcje. Zamawiający dopuszcza aby były one zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub programowych: 1. Kontrola dostępu - zapora ogniowa klasy Stateful Inspection. 2. Kontrola Aplikacji. 3. Poufność transmisji danych - połączenia szyfrowane IPSec VPN oraz SSL VPN. 4. Ochrona przed malware - co najmniej dla protokołów SMTP, POP3, IMAP, HTTP, FTP, HTTPS. 5. Ochrona przed atakami - Intrusion Prevention System. 6. Kontrola stron WWW. 7. Kontrola zawartości poczty - Antyspam dla protokołów SMTP, POP3. 8. Zarządzanie pasmem (QoS, Traffic shaping). 9. Mechanizmy ochrony przed wyciekiem poufnej informacji (DLP). 10. Dwuskładnikowe uwierzytelnianie z wykorzystaniem tokenów sprzętowych lub programowych. W ramach postępowania powinny zostać dostarczone co najmniej 2 tokeny sprzętowe lub programowe, które będą zastosowane do dwu-składnikowego uwierzytelnienia administratorów lub w ramach połączeń VPN typu client-to-site. 11. Analiza ruchu szyfrowanego protokołem SSL także dla protokołu HTTP/2. 12. Funkcja lokalnego serwera DNS ze wsparciem dla DNS over TLS (DoT) oraz DNS over HTTPS (DoH) z możliwością filtrowania zapytań DNS na lokalnym serwerze DNS jak i w ruchu przechodzącym przez system
Polityki, Firewall	1. Polityka Firewall musi uwzględniać adresy IP, użytkowników, protokoły, usługi sieciowe, aplikacje lub zbiory aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń. 2. System musi zapewniać translację adresów NAT: źródłowego i docelowego, translację PAT oraz: ▪ Translację jeden do jeden oraz jeden do wielu. ▪ Dedykowany ALG (Application Level Gateway) dla protokołu SIP. 3. W ramach systemu musi istnieć możliwość tworzenia wydzielonych stref bezpieczeństwa np. DMZ, LAN, WAN.

	4. Możliwość wykorzystania w polityce bezpieczeństwa zewnętrznych repozytoriów zawierających: kategorie url, adresy IP, nazwy domenowe, hash'e złośliwych plików. 5. Element systemu realizujący funkcję Firewall musi integrować się z następującymi rozwiązaniami SDN w celu dynamicznego pobierania informacji o zainstalowanych maszynach wirtualnych po to aby użyć ich przy budowaniu polityk kontroli dostępu. ▪ Amazon Web Services (AWS). ▪ Microsoft Azure ▪ Google Cloud Platform (GCP). ▪ OpenStack. ▪ VMware NSX.
Połączenia VPN	1. System musi umożliwiać konfigurację połączeń typu IPSec VPN. W zakresie tej funkcji musi zapewniać: ▪ Wsparcie dla IKE v1 oraz v2. ▪ Obsługa szyfrowania protokołem AES z kluczem 128 i 256 bitów w trybie pracy Galois/Counter Mode(GCM). ▪ Obsługa protokołu Diffie-Hellman grup 19 i 20. ▪ Wsparcie dla Pracy w topologii Hub and Spoke oraz Mesh, w tym wsparcie dla dynamicznego zestawiania tuneli pomiędzy SPOKE w topologii HUB and SPOKE. ▪ Tworzenie połączeń typu Site-to-Site oraz Client-to-Site. ▪ Monitorowanie stanu tuneli VPN i stałego utrzymywania ich aktywności. ▪ Możliwość wyboru tunelu przez protokoły: dynamicznego routingu (np. OSPF) oraz routingu statycznego. ▪ Obsługa mechanizmów: IPSec NAT Traversal, DPD, Xauth. ▪ Mechanizm „Split tunneling” dla połączeń Client-to-Site. 2. System musi umożliwiać konfigurację połączeń typu SSL VPN. W zakresie tej funkcji musi zapewniać: ▪ Pracę w trybie Portal - gdzie dostęp do chronionych zasobów realizowany jest za pośrednictwem przeglądarki. W tym zakresie system musi zapewniać stronę komunikacyjną działającą w oparciu o HTML 5.0. ▪ Pracę w trybie Tunnel z możliwością włączenia funkcji „Split tunneling” przy zastosowaniu dedykowanego klienta. ▪ Producent rozwiązania musi dostarczać oprogramowanie klienckie VPN, które umożliwia realizację połączeń IPSec VPN lub SSL VPN.
Routing i obsługa łączy WAN	W zakresie routingu rozwiązanie powinno zapewniać obsługę: ▪ Routingu statycznego. ▪ Policy Based Routingu.

	▪ Protokołów dynamicznego routingu w oparciu o protokoły: RIPv2, OSPF, BGP oraz PIM.
Funkcje SD-WAN	1. System powinien umożliwiać wykorzystanie protokołów dynamicznego routingu przy konfiguracji równoważenia obciążenia do łączy WAN. 2. Reguły SD-WAN powinny umożliwiać określenie aplikacji jako argumentu dla kierowania ruchu.
Zarządzanie pasmem	1. System Firewall musi umożliwiać zarządzanie pasmem poprzez określenie: maksymalnej, gwarantowanej ilości pasma, oznaczanie DSCP oraz wskazanie priorytetu ruchu. 2. Musi istnieć możliwość określania pasma dla poszczególnych aplikacji. 3. System musi zapewniać możliwość zarządzania pasmem dla wybranych kategorii URL.
Ochrona przed malware	1. Silnik antywirusowy musi umożliwiać skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021). 2. System musi umożliwiać skanowanie archiwów, w tym co najmniej: zip, RAR. 3. System musi dysponować sygnaturami do ochrony urządzeń mobilnych (co najmniej dla systemu operacyjnego Android). 4. System musi współpracować z dedykowaną platformą typu Sandbox lub usługą typu Sandbox realizowaną w chmurze. W ramach postępowania musi zostać dostarczona platforma typu Sandbox wraz z niezbędnymi serwisami lub licencja upoważniająca do korzystania z usługi typu Sandbox w chmurze. 5. System musi umożliwiać usuwanie aktywnej zawartości plików PDF oraz Microsoft Office bez konieczności blokowania transferu całych plików. 6. Możliwość wykorzystania silnika sztucznej inteligencji AI wytrenowanego przez laboratoria producenta.
Ochrona przed atakami	1. Ochrona IPS powinna opierać się co najmniej na analizie sygnaturowej oraz na analizie anomalii w protokołach sieciowych. 2. System powinien chronić przed atakami na aplikacje pracujące na niestandardowych portach. 3. Baza sygnatur ataków powinna zawierać minimum 5000 wpisów i być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora. 4. Administrator systemu musi mieć możliwość definiowania własnych wyjątków oraz własnych sygnatur. 5. System musi zapewniać wykrywanie anomalii protokołów i ruchu sieciowego, realizując tym samym podstawową ochronę przed atakami typu DoS oraz DDoS.

	6. Mechanizmy ochrony dla aplikacji Web'owych na poziomie sygnaturowym (co najmniej ochrona przed: CSS, SQL Injecton, Trojany, Exploity, Roboty) oraz możliwość kontrolowania długości nagłówka, ilości parametrów URL, Cookies. 7. Wykrywanie i blokowanie komunikacji C&C do sieci botnet.
Kontrola aplikacji	1. Funkcja Kontroli Aplikacji powinna umożliwiać kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP. 2. Baza Kontroli Aplikacji powinna zawierać minimum 2000 sygnatur i być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora. 3. Aplikacje chmurowe (co najmniej: Facebook, Google Docs, Dropbox) powinny być kontrolowane pod względem wykonywanych czynności, np.: pobieranie, wysyłanie plików. 4. Baza powinna zawierać kategorie aplikacji szczególnie istotne z punktu widzenia bezpieczeństwa: proxy, P2P. 5. Administrator systemu musi mieć możliwość definiowania wyjątków oraz własnych sygnatur.
Kontrola www	1. Moduł kontroli WWW musi korzystać z bazy zawierającej co najmniej 40 milionów adresów URL pogrupowanych w kategorie tematyczne. 2. W ramach filtra www powinny być dostępne kategorie istotne z punktu widzenia bezpieczeństwa, jak: malware (lub inne będące źródłem złośliwego oprogramowania), phishing, spam, Dynamic DNS, proxy. 3. Filtr WWW musi dostarczać kategorii stron zabronionych prawem: Hazard. 4. Administrator musi mieć możliwość nadpisywania kategorii oraz tworzenia wyjątków - białe/czarne listy dla adresów URL. 5. Funkcja Safe Search - przeciwdziałająca pojawieniu się niechcianych treści w wynikach wyszukiwarek takich jak: Google, oraz Yahoo. 6. Administrator musi mieć możliwość definiowania komunikatów zwracanych użytkownikowi dla różnych akcji podejmowanych przez moduł filtrowania. 7. W ramach systemu musi istnieć możliwość określenia, dla których kategorii url lub wskazanych url - system nie będzie dokonywał inspekcji szyfrowanej komunikacji.
Uwierzytelnianie użytkowników w ramach sesji	1. System Firewall musi umożliwiać weryfikację tożsamości użytkowników za pomocą: ▪ Haseł statycznych i definicji użytkowników przechowywanych w lokalnej bazie systemu. ▪ Haseł statycznych i definicji użytkowników przechowywanych w bazach zgodnych z LDAP.

	▪ Haseł dynamicznych (RADIUS, RSA SecurID) w oparciu o zewnętrzne bazy danych. 2. Musi istnieć możliwość zastosowania w tym procesie uwierzytelniania dwuskładnikowego. 3. Rozwiązanie powinno umożliwiać budowę architektury uwierzytelniania typu Single Sign On przy integracji ze środowiskiem Active Directory oraz zastosowanie innych mechanizmów: RADIUS lub API. 4. Uwierzytelnianie w oparciu o protokół SAML w politykach bezpieczeństwa systemu dotyczących ruchu http.
Zarządzanie	1. Elementy systemu bezpieczeństwa muszą mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH, jak i powinny mieć możliwość współpracy z dedykowanymi platformami centralnego zarządzania i monitorowania. 2. Komunikacja systemów zabezpieczeń z platformami centralnego zarządzania musi być realizowana z wykorzystaniem szyfrowanych protokołów. 3. Powinna istnieć możliwość włączenia mechanizmów uwierzytelniania dwuskładnikowego dla dostępu administracyjnego. 4. System musi współpracować z rozwiązaniami monitorowania poprzez protokoły SNMP w wersjach 2c, 3 oraz umożliwiać przekazywanie statystyk ruchu za pomocą protokołów netflow lub sflow. 5. System musi mieć możliwość zarządzania przez systemy firm trzecich poprzez API, do którego producent udostępnia dokumentację. 6. Element systemu pełniący funkcję Firewal musi posiadać wbudowane narzędzia diagnostyczne, przynajmniej: ping, traceroute, podglądu pakietów, monitorowanie procesowania sesji oraz stanu sesji firewall. 7. Element systemu realizujący funkcję firewall musi umożliwiać wykonanie szeregu zmian przez administratora w CLI lub GUI, które nie zostaną zaimplementowane zanim nie zostaną zatwierdzone.
Logowanie	1. Elementy systemu bezpieczeństwa muszą realizować logowanie do aplikacji (logowania i raportowania) udostępnianej w chmurze, lub w ramach dostawy musi zostać zapewnionyu (dostarczony) komercyjny system logowania i raportowania w postaci odpowiednio zabezpieczonej, komercyjnej platformy sprzętowej lub programowej. 2. W przypadku kiedy usługa logowania i raportowania realizowana jest w chmurze, wykonawca musi dostarczyć stosowne licencje upoważniające do składowania logów. <u>Zamawiający wymaga zapewnienia tej funkcjonalności przez okres jednego roku, w okresie realizacji projektu, tj. nie dłużej niż do 30.09.2023 r.</u>

	3. W ramach logowania system pełniący funkcję Firewall musi zapewniać przekazywanie danych o zaakceptowanym ruchu, ruchu blokowanym, aktywności administratorów, zużyciu zasobów oraz stanie pracy systemu. Musi być zapewniona możliwość jednoczesnego wysyłania logów do wielu serwerów logowania. 4. Logowanie musi obejmować zdarzenia dotyczące wszystkich modułów sieciowych i bezpieczeństwa oferowanego systemu. 5. Musi istnieć możliwość logowania do serwera SYSLOG.
Certyfikaty i normy	Poszczególne elementy oferowanego systemu bezpieczeństwa powinny posiadać następujące certyfikacje: ▪ ICSA lub EAL4 dla funkcji Firewall.
Serwisy i licencje	W ramach realizacji zadania Zamawiający wymaga dostarczenia licencji upoważniających do korzystania z aktualnych baz funkcji ochronnych producenta i serwisów. Zamawiający wymaga zapewnienia tej funkcjonalności przez okres jednego roku, w okresie realizacji projektu, tj. nie dłużej niż do 30.09.2023 r. Powinny one obejmować: 1. Kontrola Aplikacji, IPS, Antywirus (z uwzględnieniem sygnatur do ochrony urządzeń mobilnych - co najmniej dla systemu operacyjnego Android), Analiza typu Sandbox, Antyspam, Web Filtering, bazy reputacyjne adresów IP/domen 2. Licencja na usługę realizowaną w chmurze umożliwiająca logowanie i raportowanie z czasem retencji logów.
Warunki gwarancyjno-serwisowe	Gwarancja: System musi być objęty serwisem gwarancyjnym producenta przez okres 1 roku (12 miesięcy), polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości. W ramach tego serwisu producent musi zapewniać również dostęp do aktualizacji oprogramowania oraz wsparcie techniczne w trybie 24x7.
Wsparcie techniczne dla systemu Firewall	Zamawiający wymaga dostawy systemu objętego rozszerzonym wsparciem technicznym gwarantującym udostępnienie oraz dostarczenie sprzętu zastępczego na czas naprawy sprzętu w ciągu 8 godzin od momentu potwierdzenia zasadności zgłoszenia, realizowanym przez producenta rozwiązania lub autoryzowanego dystrybutora przez okres udzielonej gwarancji. Dla dostarczonego rozwiązania Wykonawca zapewni usługę wsparcia technicznego świadczoną w języku polskim przez producenta lub Autoryzowanego Partnera Serwisowego Producenta w okresie udzielonej gwarancji przez okres jednego roku, w okresie realizacji projektu, tj. nie dłużej niż do 30.09.2023 co najmniej w następującym zakresie: ▪ wsparcie telefoniczne zespołu certyfikowanych inżynierów, ▪ doradztwo w zakresie konfiguracji, ▪ zdalne wsparcie techniczne,

	▪ pomoc w zakładaniu zgłoszeń serwisowych u producenta, ▪ pomoc w procesie realizacji naprawy i wymiany w ramach gwarancji producenta, ▪ przygotowanie urządzenia do zdalnej konfiguracji, ▪ zdalna konfiguracja urządzenia (połączenia szyfrowane) zgodnie z wymaganiami użytkownika, ▪ minimum 10 zdalnych rekonfiguracji urządzenia w związku ze zmianą środowiska lub wymagań użytkownika.
Wymagania ogólne	1. W przypadku istnienia takiego wymogu w stosunku do technologii objętej przedmiotem niniejszego postępowania (tzw. produkty podwójnego zastosowania), Dostawca winien przedłożyć dokument pochodzący od importera tej technologii stwierdzający, iż przy jej wprowadzeniu na terytorium Polski, zostały dochowane wymogi właściwych przepisów prawa, w tym ustawy z dnia 29 listopada 2000 r. o obrocie z zagranicą towarami, technologiami i usługami o znaczeniu strategicznym dla bezpieczeństwa państwa, a także dla utrzymania międzynarodowego pokoju i bezpieczeństwa (Dz.U. z 2004, Nr 229, poz. 2315 z późn zm.) oraz dokument potwierdzający, że importer posiada certyfikowany przez właściwą jednostkę system zarządzania jakością tzw. wewnętrzny system kontroli wymagany dla wspólnotowego systemu kontroli wywozu, transferu, pośrednictwa i tranzytu w odniesieniu do produktów podwójnego zastosowania. 2. Oferent winien przedłożyć oświadczenie producenta lub autoryzowanego dystrybutora producenta na terenie Polski, iż oferent posiada autoryzację producenta w zakresie sprzedaży oferowanych rozwiązań.

16. DIAGNOZA CYBERBEZPIECZEŃSTWA W URZĘDZIE

MINIMALNE WYMAGANIA FUNKCJONALNE, TECHNICZNE, UŻYTKOWE, JAKOŚCIOWE
1. W ramach przedmiotu zamówienia należy wykonać diagnozę cyberbezpieczeństwa zgodnie z wymaganiami programu “Cyfrowa Gmina” oraz obowiązującymi przepisami prawa w tym zakresie. 2. Szczegółowy zakres przedmiotu diagnozy zawiera formularz informacji związanych z przeprowadzeniem diagnozy cyberbezpieczeństwa stanowiący załącznik nr 8 Regulaminu Konkursu Grantowego Cyfrowa Gmina. 3. Regulamin Konkursu Grantowego Cyfrowa Gmina wraz z formularzem - załącznikiem nr 8 został zamieszczony na stronie Centrum Projektów Polska Cyfrowa pod adresem https://www.gov.pl/web/cppc/cyfrowa-gmina.

4. Diagnoza cyberbezpieczeństwa musi zostać przeprowadzona zgodnie z Ustawą z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa oraz Rozporządzeniem Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (zwane Rozporządzeniem KRI).
5. Diagnoza musi zostać przeprowadzona przez osobę posiadającą uprawnienia wykazane w Rozporządzeniu Ministra Cyfryzacji z dnia 12 października 2018 r. w sprawie wykazu certyfikatów uprawniających do przeprowadzenia audytu w rozumieniu art. 15 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa. Wykaz certyfikatów wskazanych w w/w rozporządzeniu:
   a) Certified Internal Auditor (CIA)
   b) Certified Information System Auditor (CISA)
   c) Certyfikat audytora wiodącego systemu zarządzania bezpieczeństwem informacji według normy PN-EN ISO/IEC 27001 wydany przez jednostkę oceniającą zgodność, akredytowaną zgodnie z przepisami ustawy z dnia 13 kwietnia 2016 r. o systemach oceny zgodności i nadzoru rynku (Dz. U. z 2017 r. poz. 1398 oraz z 2018r. poz. 650 i 1138), w zakresie certyfikacji osób;
   d) Certyfikat audytora wiodącego systemu zarządzania ciągłością działania PN-EN ISO 22301 wydany przez jednostkę oceniającą zgodność, akredytowaną zgodnie z przepisami ustawy z dnia 13 kwietnia 2016 r. o systemach oceny zgodności i nadzoru rynku, w zakresie certyfikacji osób;
   e) Certified Information Security Manager (CISM);
   f) Certified in Risk and Information Systems Control (CRISC);
   g) Certified in the Governance of Enterprise IT (CGEIT);
   h) Certified Information Systems Security Professional (CISSP);
   i) Systems Security Certified Practitioner(SSCP);
   j) Certified Reliability Professional;
   k) Certyfikaty uprawniające do posiadania tytułu ISA/IEC 62443 Cybersecurity Expert.
6. Dokument końcowy musi być podpisany przez osobę posiadającą uprawnienia (wykazane w Rozporządzeniu Ministra Cyfryzacji z dnia 12 października 2018r. w sprawie wykazu certyfikatów uprawniających do przeprowadzenia audytu) raport oraz wypełniony formularz informacji związanych z przeprowadzeniem diagnozy cyberbezpieczeństwa (załącznik nr 8 do Regulaminu Konkursu Grantowego Cyfrowa Gmina) należy dostarczyć w wersji elektronicznej oraz w wersji papierowej.

Zamawiający wymaga przeprowadzenia wszystkich czynności (poza sporządzeniem raportu) objętych diagnozą cyberbezpieczeństwa w sposób stacjonarny, tj. w miejscu świadczenia usługi w siedzibie Zamawiającego w Urzędzie Gminy w Nowym Żmigrodzie.
Diagnoza musi zostać przeprowadzona w maksymalnym stopniu obiektywnie - poprzez przeprowadzone badania w Urzędzie w celu przedstawienia rzeczywistego stanu cyberbezpieczeństwa Urzędu. Zamawiający zakłada, że Wykonawca przeznaczy nie mniej niż 3 dni roboczych na wykonanie diagnozy (audytu) z tego minimum 1 dzień spędzi w Urzędzie na

prowadzenie analiz do audytu w kontakcie z wskazanymi przez Zamawiającego pracownikami urzędu.