I-I.271.11.2024 Gorzyce, 15.07.2024 r.

SPECYFIKACJA WARUNKÓW ZAMÓWIENIA

dot.: postępowania o udzielenie zamówienia publicznego. **Numer sprawy: I-I.271.11.2024**

Nazwa zadania: ***Zakup sprzętu informatycznego, oprogramowania wraz ze szkoleniami i audytami w ramach konkursu grantowego Cyberbezpieczny Samorząd.***

I. NAZWA I ADRES ZAMAWIAJĄCEGO.

Nazwa zamawiającego:	Gmina Gorzyce
Adres zamawiającego:	ul. Sandomierska 75
Kod Miejscowość:	39-432 Gorzyce
kontakt: telefon:	15-8362075
Adres strony internetowej:	http://www.bip.gminagorzyce.pl
Godziny pracy:	poniedziałek - piątek: 7.30 - 15.30.

II. STRONA INTERNETOWA PROWADZONEGO POSTĘPOWANIA.

https://platformazakupowa.pl/pn/gmina_gorzyce

III. TRYB UDZIELENIA ZAMÓWIENIA.

1. Postępowanie prowadzone jest w trybie podstawowym zgodnie z przepisami ustawy z dnia 11 września 2019 roku Prawo zamówień publicznych (Dz. U. 2023, poz. 1605) – dalej jako Pzp.
2. Postępowanie prowadzone jest w trybie podstawowym o wartości szacunkowej poniżej progów unijnych ustalonych na podstawie art. 3 Pzp.
3. Podstawa prawna wyboru trybu udzielenia zamówienia publicznego: art. 275 pkt. 1 Pzp.
4. W zakresie nieuregulowanym w niniejszej specyfikacji warunków zamówienia, zastosowanie mają przepisy Pzp.
5. Ogłoszenie zostało zamieszczone w Biuletynie Zamówień Publicznych oraz na stronie internetowej prowadzonego postępowania https://platformazakupowa.pl/pn/gmina_gorzyce.

IV. INFORMACJĘ, CZY ZAMAWIAJĄCY PRZEWIDUJE WYBÓR NAJKORZYSTNIEJSZEJ O Z MOŻLIWOŚCIĄ PROWADZENIA NEGOCJACJI.

Zamawiający nie przewiduje możliwości wyboru najkorzystniejszej oferty z możliwością przeprowadzenia negocjacji.

V. OPIS PRZEDMIOTU ZAMÓWIENIA I OPIS CZĘŚCI ZAMÓWIENIA.

1. Przedmiotem zamówienia Zakup sprzętu informatycznego, oprogramowania wraz ze szkoleniami i audytami w ramach konkursu grantowego Cyberbezpieczny Samorząd. Sprzęt składający się na przedmiot niniejszego zamówienia musi być fabrycznie nowy.

2. Z zastrzeżeniem dodatkowych postanowień poniższych niniejszego działu, opis techniczny przedmiotu niniejszego zamówienia określa Załącznik nr 2 SWZ.
3. Wspólny Słownik Zamówień CPV dla przedmiotu niniejszego zamówienia:
   a) CPV 48820000-2
   b) CPV 72268000-1
   c) CPV 72263000-6
   d) CPV 79212000-3
   e) CPV 80550000-4
4. Z zastrzeżeniem dodatkowych postanowień ust. 6 niniejszego działu, ilekroć w postanowieniach poniższych niniejszego dokumentu SWZ (i jej załącznikach), bez bliższego określenia, używany będzie zwrot SPRZĘT – należy przez to rozumieć całość sprzętu komputerowego wyszczególnionego w opisie przedmiotu zamówienia w Załączniku nr 2 SWZ, w tym oprogramowania, jeżeli w zakres Zadania w Załączniku nr 2 SWZ wchodzi również oprogramowanie.
5. Znajdujące się w Załączniku nr 2 SWZ wskazania na markę, model czy innego rodzaju oznaczenia określonego producenta mają charakter jedynie przykładowy i nie należy ich traktować jako wymagań odnoszących się do przedmiotu niniejszego zamówienia, a należy je rozpatrywać wyłącznie w kategoriach wskazań o charakterze informacyjnym (niewiążących dla Wykonawców). Zamawiający dopuszcza również zaoferowanie innego produktu, pod warunkiem, że będzie odpowiadał parametrom technicznym, funkcjonalnym i innym podobnym właściwościom minimum wskazanym dla SPRZĘTU w Załączniku nr 2 SWZ.
6. W zakres niniejszego zamówienia (realizacji dostawy, o której mowa w postanowieniach powyższych) wchodzi minimum:
   a) Sprzedaż i dostarczenie Zamawiającemu zaoferowanego SPRZĘTU z Zadania/Zadań w miejsce (zwane dalej „Miejscem Dostarczenia Sprzętu”), którym będzie wskazane przez Zamawiającego pomieszczenie w budynku Urzędu Gminy w Gorzycach, przy ul. Sandomierskiej 75, 39-432 Gorzyce (wymagane jest wniesienie sprzętu do pomieszczenia);
   b) Zapewnienie Zamawiającemu wolnej od wad prawnych licencji w odniesieniu do tych elementów SPRZĘTU w tym Zadaniu/Zadaniach, które, stosownie do Załączniku nr 2 SWZ wymagają wskazanego tam oprogramowania/innych programów komputerowych. Jeżeli treść Załącznika nr 2 SWZ nie stanowi w konkretnym przypadku inaczej zakres wymaganej licencji obejmuje licencję pełną i bezterminową;
   c) Dokonania instalacji (wdrożenia) dostarczonego Zamawiającemu w wykonaniu niniejszego zamówienia Sprzętu (Systemu), polegające na wykonaniu jego stosownego montażu (ew. spasowania, zestawienia, podłączenia);
   d) Przeprowadzenie pierwszego uruchomienia Sprzętu (Systemu), celem sprawdzenia poprawności jego działania;
   e) Udzielenie Zamawiającemu gwarancji na zaoferowany, dostarczony i wydany Zamawiającemu SPRZĘTU w Zadaniu. Wykonawca udzieli

Zamawiającemu gwarancji na SPRZĘT w Zadaniu przez okres nie krótszy niż okres wskazany dla Sprzętu w danym Zadaniu, w Załączniku nr 2 SWZ.

f) Uwaga: tam gdzie w poszczególnych Zadaniach w Załączniku nr 2 SWZ gwarancja nie została określona, minimalny termin gwarancji wynosi 24 miesiące.

g) Dokumentu gwarancyjnego na okoliczność udzielenia Zamawiającemu gwarancji, której mowa powyżej (w zakresie wynikającym ze złożonej oferty),

h) Instrukcji korzystania i poprawnej eksploatacji (w tym ewentualnie serwisowania i konserwacji) SPRZĘTU,

i) Inne dokumenty, jeżeli są niezbędne do korzystania ze Sprzętu lub zostały wymienione w Załączniku nr 2 SWZ lub Wzorze Umowy wymaganym dla danego Zadania na podstawie działu XIX ust. 1 SWZ jako dokumenty do wydania Zamawiającemu na etapie odbioru SPRZĘTU

7. Zamawiający dopuszcza zastosowanie przez Wykonawcę rozwiązań równoważnych rozwiązaniom wskazanym przez Zamawiającego. Wykonawca oferując rozwiązanie równoważne do opisanego powyżej jest zobowiązany wykazać (udowodnić) równoważność w zakresie wskazanych parametrów, które muszą być na poziomie nie gorszym niż parametry wskazane przez Zamawiającego - Wykonawca musi wykazać (udowodnić), iż proponowane rozwiązanie w równoważnym stopniu spełnia wymagania określone w zapytaniu ofertowym, w szczególności w zakresie parametrów. Jeżeli w opisie przedmiotu zamówienia znajdują się jakiekolwiek odniesienia do określonego wyrobu, źródła, znaków towarowych, patentów czy pochodzenia lub szczególnego procesu, który charakteryzuje produkty lub usługi dostarczane przez konkretnego wykonawcę – należy przyjąć, że Zamawiający podał taki opis ze wskazaniem na typ i dopuszcza składanie ofert równoważnych, w szczególności o parametrach technicznych, użytkowych, funkcjonalnych i jakościowych nie gorszych niż te, podane w opisie przedmiotu zamówienia.

VI. TERMIN WYKONANIA ZAMÓWIENIA.

Zamówienie będzie wykonane w miejscu siedziby zamawiającego. Dostawy sprzętu będą realizowane w ciągu 7 dni, wdrożenia w ciągu 90 dni, szkolenia w ciągu 90 dni, audyty w ciągu 90 dni od dnia podpisania umowy.

VII. PROJEKTOWANE POSTANOWIENIA UMOWY W SPRAWIE ZAMÓWIENIA PUBLICZNEGO, KTÓRE ZOSTANĄ WPROWADZONE DO TREŚCI TEJ UMOWY.

1. Postanowienia umowy zawarto we wzorze umowy, który stanowi załącznik nr 7 do SWZ.

I-I.271.11.2024 Gorzyce, 15.07.2024 r.

VIII. INFORMACJA O ŚRODKACH KOMUNIKACJI ELEKTRONICZNEJ, PRZY UŻYCIU KTÓRYCH ZAMAWIAJĄCY BĘDZIE KOMUNIKOWAŁ SIĘ Z WYKONAWCAMI, ORAZ INFORMACJE O WYMAGANIACH TECHNICZNYCH I ORGANIZACYJNYCH SPORZĄDZANIA, WYSYŁANIA I ODBIERANIA KORESPONDENCJI ELEKTRONICZNEJ.

1. Postępowanie prowadzone jest w języku polskim za pośrednictwem platformazakupowa.pl pod adresem[1]: https://platformazakupowa.pl/pn/gmina_gorzyce
2. W celu skrócenia czasu udzielenia odpowiedzi na pytania komunikacja między zamawiającym a wykonawcami w zakresie:
   a) przesyłania Zamawiającemu pytań do treści SWZ;
   b) przesyłania odpowiedzi na wezwanie Zamawiającego do złożenia podmiotowych środków dowodowych;
   c) przesyłania odpowiedzi na wezwanie Zamawiającego do złożenia/poprawienia/uzupełnienia oświadczenia, o którym mowa w art. 125 ust. 1, podmiotowych środków dowodowych, innych dokumentów lub oświadczeń składanych w postępowaniu;
   d) przesyłania odpowiedzi na wezwanie Zamawiającego do złożenia wyjaśnień dotyczących treści oświadczenia, o którym mowa w art. 125 ust. 1 lub złożonych podmiotowych środków dowodowych lub innych dokumentów lub oświadczeń składanych w postępowaniu;
   e) przesyłania odpowiedzi na wezwanie Zamawiającego do złożenia wyjaśnień dot. treści przedmiotowych środków dowodowych;
   f) przesłania odpowiedzi na inne wezwania Zamawiającego wynikające z ustawy - Prawo zamówień publicznych;
   g) przesyłania wniosków, informacji, oświadczeń Wykonawcy;
   h) przesyłania odwołania/inne

   odbywa się za pośrednictwem platformazakupowa.pl i formularza „Wyślij wiadomość do zamawiającego”.
3. Za datę przekazania (wpływu) oświadczeń, wniosków, zawiadomień oraz informacji przyjmuje się datę ich przesłania za pośrednictwem platformazakupowa.pl poprzez kliknięcie przycisku „Wyślij wiadomość do zamawiającego” po których pojawi się komunikat, że wiadomość została wysłana do zamawiającego.
4. Zamawiający będzie przekazywał wykonawcom informacje za pośrednictwem platformazakupowa.pl. Informacje dotyczące odpowiedzi na pytania, zmiany specyfikacji, zmiany terminu składania i otwarcia ofert Zamawiający będzie

[1] Wstawić adres Profilu Nabywcy na platformazakupowa.pl lub jeśli jednostka nie posiada wykupionego Profilu Nabywcy można dodać link do konkretnego postępowania lub ogólnie do strony platformazakupowa.pl

zamieszczał na platformie w sekcji “Komunikaty”. Korespondencja, której zgodnie z obowiązującymi przepisami adresatem jest konkretny wykonawca, będzie przekazywana za pośrednictwem platformazakupowa.pl do konkretnego wykonawcy.

5. Wykonawca jako podmiot profesjonalny ma obowiązek sprawdzania komunikatów i wiadomości bezpośrednio na platformazakupowa.pl przesłanych przez zamawiającego, gdyż system powiadomień może ulec awarii lub powiadomienie może trafić do folderu SPAM.
6. Zamawiający, zgodnie z Rozporządzeniem Prezesa Rady Ministrów z dnia 30 grudnia 2020r. w sprawie sposobu sporządzania i przekazywania informacji oraz wymagań technicznych dla dokumentów elektronicznych oraz środków komunikacji elektronicznej w postępowaniu o udzielenie zamówienia publicznego lub konkursie (Dz. U. z 2020r. poz. 2452), określa niezbędne wymagania sprzętowo - aplikacyjne umożliwiające pracę na platformazakupowa.pl, tj.:
   a) stały dostęp do sieci Internet o gwarantowanej przepustowości nie mniejszej niż 512 kb/s,
   b) komputer klasy PC lub MAC o następującej konfiguracji: pamięć min. 2 GB Ram, procesor Intel IV 2 GHZ lub jego nowsza wersja, jeden z systemów operacyjnych - MS Windows 7, Mac Os x 10 4, Linux, lub ich nowsze wersje,
   c) zainstalowana dowolna, inna przeglądarka internetowa niż Internet Explorer,
   d) włączona obsługa JavaScript,
   e) zainstalowany program Adobe Acrobat Reader lub inny obsługujący format plików .pdf,
   f) Szyfrowanie na platformazakupowa.pl odbywa się za pomocą protokołu TLS 1.3.
   g) Oznaczenie czasu odbioru danych przez platformę zakupową stanowi datę oraz dokładny czas (hh:mm:ss) generowany wg. czasu lokalnego serwera synchronizowanego z zegarem Głównego Urzędu Miar.
7. Wykonawca, przystępując do niniejszego postępowania o udzielenie zamówienia publicznego:
   a) akceptuje warunki korzystania z platformazakupowa.pl określone w Regulaminie zamieszczonym na stronie internetowej pod linkiem w zakładce „Regulamin" oraz uznaje go za wiążący,
   b) zapoznał i stosuje się do Instrukcji składania ofert/wniosków dostępnej pod linkiem.
8. Zamawiający nie ponosi odpowiedzialności za złożenie oferty w sposób niezgodny z Instrukcją korzystania z platformazakupowa.pl, w szczególności za sytuację, gdy zamawiający zapozna się z treścią oferty przed upływem terminu składania ofert (np. złożenie oferty w zakładce „Wyślij wiadomość do zamawiającego”).
   Taka oferta zostanie uznana przez Zamawiającego za ofertę handlową i nie

będzie brana pod uwagę w przedmiotowym postępowaniu ponieważ nie został spełniony obowiązek narzucony w art. 221 Ustawy Prawo Zamówień Publicznych.

9. Zamawiający informuje, że instrukcje korzystania z platformazakupowa.pl dotyczące w szczególności logowania, składania wniosków o wyjaśnienie treści SWZ, składania ofert oraz innych czynności podejmowanych w niniejszym postępowaniu przy użyciu platformazakupowa.pl znajdują się w zakładce „Instrukcje dla Wykonawców" na stronie internetowej pod adresem: https://platformazakupowa.pl/strona/45-instrukcje

Zalecenia

1. Formaty plików wykorzystywanych przez wykonawców powinny być zgodne z Obwieszczeniem Prezesa Rady Ministrów z dnia 9 listopada 2017 r. w sprawie ogłoszenia jednolitego tekstu rozporządzenia Rady Ministrów w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych.
2. Poniżej przedstawiamy listę sugerowanych zapisów do specyfikacji:
   a) Zamawiający rekomenduje wykorzystanie formatów: .pdf .doc .xls .jpg (.jpeg) ze szczególnym wskazaniem na .pdf .
   b) W celu ewentualnej kompresji danych Zamawiający rekomenduje wykorzystanie jednego z formatów:
      1. .zip;
      2. .7Z.
   c) Wśród formatów powszechnych a NIE występujących w rozporządzeniu występują: .rar .gif .bmp .numbers .pages. Dokumenty złożone w takich plikach zostaną uznane za złożone nieskutecznie.
   d) Zamawiający zwraca uwagę na ograniczenia wielkości plików podpisywanych profilem zaufanym, który wynosi max 10MB, oraz na ograniczenie wielkości plików podpisywanych w aplikacji eDoApp służącej do składania podpisu osobistego, który wynosi max 5MB.
   e) Ze względu na niskie ryzyko naruszenia integralności pliku oraz łatwiejszą weryfikację podpisu, zamawiający zaleca, w miarę możliwości, przekonwertowanie plików składających się na ofertę na format .pdf i opatrzenie ich podpisem kwalifikowanym PAdES.
   f) Pliki w innych formatach niż PDF zaleca się opatrzyć zewnętrznym podpisem XAdES. Wykonawca powinien pamiętać, aby plik z podpisem przekazywać łącznie z dokumentem podpisywanym.
   g) Zamawiający zaleca aby w przypadku podpisywania pliku przez kilka osób, stosować podpisy tego samego rodzaju. Podpisywanie różnymi rodzajami podpisów np. osobistym i kwalifikowanym może doprowadzić do problemów w weryfikacji plików.

h) Zamawiający zaleca, aby Wykonawca z odpowiednim wyprzedzeniem przetestował możliwość prawidłowego wykorzystania wybranej metody podpisania plików oferty.
i) Zaleca się, aby komunikacja z wykonawcami odbywała się tylko na Platformie za pośrednictwem formularza "Wyślij wiadomość do zamawiającego", nie za pośrednictwem adresu email.
j) Osobą składającą ofertę powinna być osoba kontaktowa podawana w dokumentacji.
k) Ofertę należy przygotować z należytą starannością dla podmiotu ubiegającego się o udzielenie zamówienia publicznego i zachowaniem odpowiedniego odstępu czasu do zakończenia przyjmowania ofert/wniosków. Sugerujemy złożenie oferty na 24 godziny przed terminem składania ofert/wniosków.
l) Podczas podpisywania plików zaleca się stosowanie algorytmu skrótu SHA2 zamiast SHA1.
m) Jeśli wykonawca pakuje dokumenty np. w plik ZIP zalecamy wcześniejsze podpisanie każdego ze skompresowanych plików.
n) Zamawiający rekomenduje wykorzystanie podpisu z kwalifikowanym znacznikiem czasu.
o) Zamawiający zaleca aby nie wprowadzać jakichkolwiek zmian w plikach po podpisaniu ich podpisem kwalifikowanym. Może to skutkować naruszeniem integralności plików co równoważne będzie z koniecznością odrzucenia oferty w postępowaniu.

IX. INFORMACJE O SPOSOBIE KOMUNIKOWANIA SIĘ ZAMAWIAJĄCEGO Z WYKONAWCAMI W INNY SPOSÓB NIŻ PRZY UŻYCIU ŚRODKÓW KOMUNIKACJI ELEKTRONICZNEJ W PRZYPADKU ZAISTNIENIA JEDNEJ Z SYTUACJI OKREŚLONYCH W ART. 65 UST. 1, ART. 66 I ART. PZP.

Zamawiający nie przewiduje komunikowania się Zamawiającego z wykonawcami w inny sposób niż przy użyciu środków komunikacji elektronicznej.

X. WSKAZANIE OSÓB UPRAWNIONYCH DO KOMUNIKOWANIA SIĘ Z WYKONAWCAMI.

Zamawiający wyznacza następujące osoby do kontaktu z Wykonawcami:
a) Krzysztof Bartoszek - przetargi-gorzyce@gminagorzyce.pl,

XI. TERMIN ZWIĄZANIA OFERTĄ.

1. Wykonawca jest związany ofertą przez okres 30 dni od dnia upływu terminu składania ofert, tj. do dnia 21.08.2024 r., określonego w rozdziale XIII ust. 2, przy czym pierwszym dniem terminu związania ofertą jest dzień, w którym upływa termin składania ofert. W przypadku gdy wybór najkorzystniejszej oferty nie nastąpi przed upływem terminu związania ofertą określonego w dokumentach zamówienia, zamawiający przed upływem terminu związania ofertą zwraca się jednokrotnie do wykonawców o wyrażenie zgody na

przedłużenie tego terminu o wskazywany przez niego okres, nie dłuższy niż 30 dni.

2. Przedłużenie terminu związania ofertą, o którym mowa w ust. 2, wymaga złożenia przez wykonawcę pisemnego oświadczenia o wyrażeniu zgody na przedłużenie terminu związania ofertą.

XII. OPIS SPOSOBU PRZYGOTOWANIA OFERTY.

1. Przygotowanie oferty.
   a) Wykonawca może złożyć jedną ofertę w języku polskim.
   b) Koszty związane z przygotowaniem oferty ponosi składający ofertę.
   c) Oferta oraz wymagane formularze, zestawienia i wykazy składane wraz z ofertą wymagają podpisu osób uprawnionych do reprezentowania firmy w obrocie gospodarczym, zgodnie z aktem rejestracyjnym oraz przepisami prawa.
   d) Oferta podpisana przez upoważnionego przedstawiciela Wykonawcy wymaga załączenia właściwego pełnomocnictwa lub umocowania prawnego.
2. Postanowienia dotyczące wnoszenia oferty wspólnej przez dwa lub więcej podmioty gospodarcze (konsorcja/spółki cywilne):
   a) Wykonawcy mogą wspólnie ubiegać się o udzielenie zamówienia.
   b) W przypadku, o którym mowa w ust. 1, wykonawcy ustanawiają pełnomocnika do reprezentowania ich w postępowaniu o udzielenie zamówienia albo do reprezentowania w postępowaniu i zawarcia umowy w sprawie zamówienia publicznego.
   c) Zamawiający nie może wymagać od wykonawców wspólnie ubiegających się o udzielenie zamówienia posiadania określonej formy prawnej w celu złożenia oferty w postępowaniu.
   d) W odniesieniu do wykonawców wspólnie ubiegających się o udzielenie zamówienia zamawiający może określić wymagania związane z realizacją zamówienia w inny sposób niż w odniesieniu do pojedynczych wykonawców, jeżeli jest to uzasadnione charakterem zamówienia i proporcjonalne do jego przedmiotu.
   e) Przepisy dotyczące wykonawcy stosuje się odpowiednio do wykonawców wspólnie ubiegających się o udzielenie zamówienia.
   f) Jeżeli została wybrana oferta wykonawców wspólnie ubiegających się o udzielenie zamówienia, zamawiający może żądać przed zawarciem umowy w sprawie zamówienia publicznego kopii umowy regulującej współpracę tych wykonawców.

XIII. SPOSÓB ORAZ TERMIN SKŁADANIA OFERT.

1. Oferta, wniosek oraz przedmiotowe środki dowodowe (jeżeli były wymagane) składane elektronicznie muszą zostać podpisane elektronicznym kwalifikowanym podpisem lub podpisem zaufanym lub podpisem osobistym.

W procesie składania oferty, wniosku w tym przedmiotowych środków dowodowych na platformie, kwalifikowany podpis elektroniczny lub podpis zaufany lub podpis osobisty Wykonawca składa bezpośrednio na dokumencie, który następnie przesyła do systemu.

2. Poświadczenia za zgodność z oryginałem dokonuje odpowiednio wykonawca, podmiot, na którego zdolnościach lub sytuacji polega wykonawca, wykonawcy wspólnie ubiegający się o udzielenie zamówienia publicznego albo podwykonawca, w zakresie dokumentów, które każdego z nich dotyczą. Poprzez oryginał należy rozumieć dokument podpisany kwalifikowanym podpisem elektronicznym lub podpisem zaufanym lub podpisem osobistym przez osobę/osoby upoważnioną/upoważnione. Poświadczenie za zgodność z oryginałem następuje w formie elektronicznej podpisane kwalifikowanym podpisem elektronicznym lub podpisem zaufanym lub podpisem osobistym przez osobę/osoby upoważnioną/upoważnione.
3. Oferta powinna być:
4. sporządzona na podstawie załączników niniejszej SWZ w języku polskim,
5. złożona przy użyciu środków komunikacji elektronicznej tzn. za pośrednictwem platformazakupowa.pl,
6. podpisana kwalifikowanym podpisem elektronicznym lub podpisem zaufanym lub podpisem osobistym przez osobę/osoby upoważnioną/upoważnione
7. Podpisy kwalifikowane wykorzystywane przez wykonawców do podpisywania wszelkich plików muszą spełniać “Rozporządzenie Parlamentu Europejskiego i Rady w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym (eIDAS) (UE) nr 910/2014 - od 1 lipca 2016 roku”.
8. W przypadku wykorzystania formatu podpisu XAdES zewnętrzny. Zamawiający wymaga dołączenia odpowiedniej ilości plików tj. podpisywanych plików z danymi oraz plików podpisu w formacie XAdES.
9. Zgodnie z art. 18 ust. 3 ustawy Pzp, nie ujawnia się informacji stanowiących tajemnicę przedsiębiorstwa, w rozumieniu przepisów o zwalczaniu nieuczciwej konkurencji. Jeżeli wykonawca, nie później niż w terminie składania ofert, w sposób niebudzący wątpliwości zastrzegł, że nie mogą być one udostępniane oraz wykazał, załączając stosowne wyjaśnienia, iż zastrzeżone informacje stanowią tajemnicę przedsiębiorstwa. Na platformie w formularzu składania oferty znajduje się miejsce wyznaczone do dołączenia części oferty stanowiącej tajemnicę przedsiębiorstwa.
10. Wykonawca, za pośrednictwem platformazakupowa.pl może przed upływem terminu składania ofert wycofać ofertę. Sposób dokonywania wycofania oferty zamieszczono w instrukcji zamieszczonej na stronie internetowej pod adresem: https://platformazakupowa.pl/strona/45-instrukcje
11. Każdy z wykonawców może złożyć tylko jedną ofertę. Złożenie większej liczby ofert lub oferty zawierającej propozycje wariantowe podlegać będą odrzuceniu.

12. Ceny oferty muszą zawierać wszystkie koszty, jakie musi ponieść wykonawca, aby zrealizować zamówienie z najwyższą starannością oraz ewentualne rabaty.
13. Dokumenty i oświadczenia składane przez wykonawcę powinny być w języku polskim, chyba że w SWZ dopuszczono inaczej. W przypadku załączenia dokumentów sporządzonych w innym języku niż dopuszczony, wykonawca zobowiązany jest załączyć tłumaczenie na język polski.
14. Zgodnie z definicją dokumentu elektronicznego z art.3 ustęp 2 Ustawy o informatyzacji działalności podmiotów realizujących zadania publiczne, opatrzenie pliku zawierającego skompresowane dane kwalifikowanym podpisem elektronicznym jest jednoznaczne z podpisaniem oryginału dokumentu, z wyjątkiem kopii poświadczonych odpowiednio przez innego wykonawcę ubiegającego się wspólnie z nim o udzielenie zamówienia, przez podmiot, na którego zdolnościach lub sytuacji polega wykonawca, albo przez podwykonawcę.
15. Maksymalny rozmiar jednego pliku przesyłanego za pośrednictwem dedykowanych formularzy do: złożenia, zmiany, wycofania oferty wynosi 150 MB natomiast przy komunikacji wielkość pliku to maksymalnie 500 MB.
16. Ofertę wraz z wymaganymi dokumentami należy umieścić na platformazakupowa.pl pod adresem: https://platformazakupowa.pl/pn/gmina_gorzyce w myśl Ustawy na stronie internetowej prowadzonego postępowania do dnia 23.07.2024 r. do godziny 09:00.

XIV. TERMIN OTWARCIA OFERT.

1. Otwarcie ofert nastąpi w dniu 23.07.2024 r., o godzinie 09:30
2. Niezwłocznie po otwarciu ofert Zamawiający udostępni na stronie internetowej prowadzonego postępowania informacje o: (1) nazwach albo imionach i nazwiskach oraz siedzibach lub miejscach prowadzonej działalności gospodarczej albo miejscach zamieszkania wykonawców, których oferty zostały otwarte; (2) cenach lub kosztach zawartych w ofertach.
3. Otwarcie ofert nastąpi niezwłocznie po upływie terminu składania ofert.
4. Jeżeli otwarcie ofert następuje przy użyciu systemu teleinformatycznego, w przypadku awarii tego systemu, która powoduje brak możliwości otwarcia ofert w terminie określonym przez zamawiającego, otwarcie ofert następuje niezwłocznie po usunięciu awarii.
5. Zamawiający informuje o zmianie terminu otwarcia ofert na stronie internetowej prowadzonego postępowania.
6. Zamawiający, najpóźniej przed otwarciem ofert, udostępnia na stronie internetowej prowadzonego postępowania informację o kwocie, jaką zamierza przeznaczyć na sfinansowanie zamówienia.
7. Zamawiający, niezwłocznie po otwarciu ofert, udostępnia na stronie internetowej prowadzonego postępowania informacje o:

8. nazwach albo imionach i nazwiskach oraz siedzibach lub miejscach prowadzonej działalności gospodarczej albo miejscach zamieszkania wykonawców, których oferty zostały otwarte;
9. cenach lub kosztach zawartych w ofertach.
10. W przypadku ofert, które podlegają negocjacjom, zamawiający udostępnia informacje, o których mowa ust. 9 pkt 2, niezwłocznie po otwarciu ofert ostatecznych albo unieważnieniu postępowania.
11. Do oferty należy dołączyć wszystkie wymagane w SWZ dokumenty. Po wypełnieniu Formularza składania oferty lub wniosku i dołączenia wszystkich wymaganych załączników należy kliknąć przycisk „Przejdź do podsumowania".
12. Oferta lub wniosek składana elektronicznie musi zostać podpisana elektronicznym podpisem kwalifikowanym, podpisem zaufanym lub podpisem osobistym. W procesie składania oferty za pośrednictwem platformazakupowa.pl, wykonawca powinien złożyć podpis bezpośrednio na dokumentach przesłanych za pośrednictwem platformazakupowa.pl. Zalecamy stosowanie podpisu na każdym załączonym pliku osobno, w szczególności wskazanych w art. 63 ust 1 oraz ust.2 Pzp, gdzie zaznaczono, iż oferty, wnioski o dopuszczenie do udziału w postępowaniu oraz oświadczenie, o którym mowa w art. 125 ust.1 sporządza się, pod rygorem nieważności, w postaci lub formie elektronicznej i opatruje się odpowiednio w odniesieniu do wartości postępowania kwalifikowanym podpisem elektronicznym, podpisem zaufanym lub podpisem osobistym.
13. Za datę złożenia oferty przyjmuje się datę jej przekazania w systemie (platformie) w drugim kroku składania oferty poprzez kliknięcie przycisku "Złóż ofertę" i wyświetlenie się komunikatu, że oferta została zaszyfrowana i złożona.
14. Szczegółowa instrukcja dla Wykonawców dotycząca złożenia, zmiany i wycofania oferty znajduje się na stronie internetowej pod adresem: https://platformazakupowa.pl/strona/45-instrukcje

XV. PODSTAWY WYKLUCZENIA, O KTÓRYCH MOWA W ART. 108 UST. 1. PZP:

1. Z postępowania o udzielenie zamówienia wyklucza się wykonawcę:
   a) będącego osobą fizyczną, którego prawomocnie skazano za przestępstwo:
   b) udziału w zorganizowanej grupie przestępczej albo związku mającym na celu popełnienie przestępstwa lub przestępstwa skarbowego, o którym mowa w art. 258 Kodeksu karnego,
   c) handlu ludźmi, o którym mowa w art. 189a Kodeksu karnego,
   d) o którym mowa w art. 228-230a, art. 250a Kodeksu karnego lub w art. 46 lub art. 48 ustawy z dnia 25 czerwca 2010 r. o sporcie,
   e) finansowania przestępstwa o charakterze terrorystycznym, o którym mowa w art. 165a Kodeksu karnego, lub przestępstwo udaremniania lub utrudniania stwierdzenia przestępnego pochodzenia pieniędzy lub ukrywania ich pochodzenia, o którym mowa w art. 299 Kodeksu karnego,
   f) o charakterze terrorystycznym, o którym mowa w art. 115 § 20 Kodeksu karnego, lub mające na celu popełnienie tego przestępstwa,

g) powierzenia wykonywania pracy małoletniemu cudzoziemcowi, o którym mowa w art. 9 ust. 2 ustawy z dnia 15 czerwca 2012 r. o skutkach powierzania wykonywania pracy cudzoziemcom przebywającym wbrew przepisom na terytorium Rzeczypospolitej Polskiej (Dz. U. poz. 769),

h) przeciwko obrotowi gospodarczemu, o których mowa w art. 296-307 Kodeksu karnego, przestępstwo oszustwa, o którym mowa w art. 286 Kodeksu karnego, przestępstwo przeciwko wiarygodności dokumentów, o których mowa w art. 270-277d Kodeksu karnego, lub przestępstwo skarbowe, o którym mowa w art. 9 ust. 1 i 3 lub art. 10 ustawy z dnia 15 czerwca 2012 r. o skutkach powierzania wykonywania pracy cudzoziemcom przebywającym wbrew przepisom na terytorium Rzeczypospolitej Polskiej

lub za odpowiedni czyn zabroniony określony w przepisach prawa obcego;

2. jeżeli urzędującego członka jego organu zarządzającego lub nadzorczego, wspólnika spółki w spółce jawnej lub partnerskiej albo komplementariusza w spółce komandytowej lub komandytowo-akcyjnej lub prokurenta prawomocnie skazano za przestępstwo, o którym mowa w pkt 1.
3. wobec którego wydano prawomocny wyrok sądu lub ostateczną decyzję administracyjną o zaleganiu z uiszczeniem podatków, opłat lub składek na ubezpieczenie społeczne lub zdrowotne, chyba że wykonawca przed upływem terminu składania ofert dokonał płatności należnych podatków, opłat lub składek na ubezpieczenie społeczne lub zdrowotne wraz z odsetkami lub grzywnami lub zawarł wiążące porozumienie w sprawie spłaty tych należności;
4. wobec którego prawomocnie orzeczono zakaz ubiegania się o zamówienia publiczne;
5. jeżeli zamawiający może stwierdzić, na podstawie wiarygodnych przesłanek, że wykonawca zawarł z innymi wykonawcami porozumienie mające na celu zakłócenie konkurencji, w szczególności jeżeli należąc do tej samej grupy kapitałowej w rozumieniu ustawy z dnia 16 lutego 2007 r. o ochronie konkurencji i konsumentów, złożyli odrębne oferty, oferty częściowe, chyba że wykażą, że przygotowali te oferty niezależnie od siebie;
6. jeżeli, w przypadkach, o których mowa w art. 85 ust. 1, doszło do zakłócenia konkurencji wynikającego z wcześniejszego zaangażowania tego wykonawcy lub podmiotu, który należy z wykonawcą do tej samej grupy kapitałowej w rozumieniu ustawy z dnia 16 lutego 2007 r. o ochronie konkurencji i konsumentów, chyba że spowodowane tym zakłócenie konkurencji może być wyeliminowane w inny sposób niż przez wykluczenie wykonawcy z udziału w postępowaniu o udzielenie zamówienia.

XVI. SPOSÓB OBLICZENIA CENY.

1. Cena oferty jest wynagrodzeniem ryczałtowym i uwzględnia wszystkie zobowiązania, musi być podana w PLN cyfrowo i słownie, z wyodrębnieniem należnego podatku VAT - jeżeli występuje.

2. Cena podana w ofercie winna obejmować wszystkie koszty i składniki związane z wykonaniem zamówienia.
3. Cena może być tylko jedna za oferowany przedmiot zamówienia.
4. Nie dopuszcza się wariantowości cen.
5. Cena nie ulega zmianie przez okres ważności oferty (związania ofertą).

XVII. OPIS KRYTERIÓW OCENY OFERT, WRAZ Z PODANIEM WAG TYCH KRYTERIÓW, I SPOSOBU OCENY OFERT.

1. Przy wyborze oferty Zamawiający będzie się kierował następującymi kryteriami:

Lp.	Nazwa kryterium	Waga (pkt)
1.	Cena (całkowity koszt wykonania zamówienia)	60
2.	Możliwość wykonania zamówienia poza godzinami pracy urzędu, także w soboty i niedziele	40

2. Przy wyborze oferty Zamawiający będzie stosować zasadę, że oferta nieodrzucona, zawierająca najwyższą liczbę punktów przyznanych według powyższych kryteriów, jest ofertą najkorzystniejszą.
3. W toku dokonywania badania i oceny ofert Zamawiający może żądać udzielenia przez Wykonawców wyjaśnień treści złożonych przez nich ofert.
4. Przy ocenie ofert w kryterium „Cena” (C) punkty zostaną przyznane w poniższy sposób:
   - Cena – znaczenie 60% (maksymalnie do 60 pkt)
   - Kryterium ceny będzie rozpatrywane na podstawie ceny brutto podanej przez Wykonawcę w Formularzu Ofertowym.
   - Punkty w kryterium „Cena” będą obliczane na podstawie wzoru:

C = CC min/ CC of x 60

gdzie:

C – punkty przyznane Wykonawcy w ramach kryterium „Cena”

CC min – najniższa cena brutto spośród badanych ofert

CC of – cena brutto badanej ofert

   - Do wzoru zostaną przyjęte ceny podane przez Wykonawców w Formularzu Oferty stanowiącym Załącznik nr 1 do SWZ.
5. Kryterium „Możliwość wykonania zamówienia poza godzinami pracy urzędu, także w soboty i niedziele” stanowi 40 możliwych do uzyskania punktów.
6. Sumaryczna liczba punktów zostanie obliczona według wzoru:

   W = C + E

   gdzie:

   W – łączna liczba punktów przyznanych w poszczególnych kryteriach,

C – liczba punktów przyznanych w kryterium „Cena”,

E – wartość punktowa kryterium „Możliwość wykonania zamówienia poza godzinami pracy urzędu, także w soboty i niedziele”,

7. Wszystkie obliczenia dokonywane będą z dokładnością do dwóch miejsc po przecinku.

XVIII. INFORMACJE O FORMALNOŚCIACH, JAKIE MUSZĄ ZOSTAĆ DOPEŁNIONE PO WYBORZE OFERTY W CELU ZAWARCIA UMOWY W SPRAWIE ZAMÓWIENIA PUBLICZNEGO.

1. Umowa w sprawie realizacji zamówienia publicznego zawarta zostanie z uwzględnieniem postanowień wynikających z treści niniejszej SWZ oraz danych zawartych w ofercie.
2. Zamawiający podpisze umowę z Wykonawcą, który złoży najkorzystniejszą ofertę.
3. Zamawiający niezwłocznie po wyborze najkorzystniejszej oferty zawiadomi Wykonawców podając w szczególności:
   a) nazwę (firmę) i adres Wykonawcy, którego ofertę wybrano, oraz uzasadnienie jej wyboru, a także nazwy (firmy), siedziby i adresy Wykonawców, którzy złożyli oferty, wraz ze streszczeniem oceny i porównania złożonych ofert zawierającym punktację przyznaną ofertom w każdym kryterium oceny ofert i łączną punktację;
   b) uzasadnienie faktyczne i prawne wykluczenia Wykonawców, jeżeli takie będzie miało miejsce;
   c) uzasadnienie faktyczne i prawne odrzucenia ofert, jeżeli takie będzie miało miejsce.
4. O unieważnieniu postępowania o udzielenie zamówienia publicznego Zamawiający zawiadomi równocześnie wszystkich Wykonawców, którzy:
   a) ubiegali się o udzielenie zamówienia - w przypadku unieważnienia postępowania przed upływem terminu składania ofert,
   b) złożyli oferty - w przypadku unieważnienia postępowania po upływie terminu składania ofert podając uzasadnienie faktyczne i prawne.
5. W przypadku unieważnienia postępowania o udzielenie zamówienia, Zamawiający na wniosek Wykonawcy, który ubiegał się o udzielenie zamówienia, zawiadomi o wszczęciu kolejnego postępowania, które dotyczy tego samego przedmiotu zamówienia lub obejmuje ten sam przedmiot zamówienia.
6. Umowa zostanie zawarta w formie pisemnej po upływie wymaganych terminu przewidzianego chyba, że w postępowaniu została złożona tylko jedna oferta, w takim przypadku umowa może zostać podpisana przed upływem tego terminu.
7. O miejscu i terminie podpisania umowy Zamawiający powiadomi wybranego Wykonawcę.
8. W przypadku, gdy okaże się, że Wykonawca, którego oferta została wybrana będzie uchylał się od zawarcia umowy Zamawiający może wybrać ofertę najkorzystniejszą spośród pozostałych ofert, bez przeprowadzania ich

ponownej oceny, chyba, że zachodzi jedna z przesłanek unieważnienia postępowania.

XIX. POUCZENIE O ŚRODKACH OCHRONY PRAWNEJ PRZYSŁUGUJĄCYCH WYKONAWCY.

1. Wykonawcy przysługują środki ochrony prawnej zgodnie z działem IX Pzp.

XX. INFORMACJĘ O WARUNKACH UDZIAŁU W POSTĘPOWANIU.

1. Warunki udziału w postępowaniu:
   a) zdolności do występowania w obrocie gospodarczym – Zamawiający nie wyznacza szczegółowego warunku w tym zakresie;
   b) uprawnień do prowadzenia określonej działalności gospodarczej lub zawodowej, o ile wynika to z odrębnych przepisów – Zamawiający nie wyznacza szczegółowego warunku w tym zakresie;
   c) sytuacji ekonomicznej lub finansowej – Zamawiający nie wyznacza szczegółowego warunku w tym zakresie;
   d) zdolności technicznej lub zawodowej - Wykonawca jest zobowiązany do wykazania kompetencji niezbędnych do realizacji niniejszego zamówienia poprzez złożenie kopii następujących certyfikatów:
      - co najmniej dwa z trzech certyfikatów: MS 50255 Managing, Maintaining, and Securing Your Networks Through Group Policy, SC-900 Microsoft Certified: Security, Compliance, and Identity Fundamentals, MS-55341 Installation, Storage, and Compute with Windows Server, w zakresie usług i rozwiązań opartych o środowisko Microsoft;
      - ITIL® Foundation Certificate in IT Service Management w zakresie projektowania, zrozumienia i zastosowania najlepszych praktyk w zarządzaniu usługami informatycznymi;
      - co najmniej dwa z trzech certyfikatów: Offensive Security Certified Professional (OSCP), Offensive Security Certified Expert (OSCE), Certified Professional Penetration Tester (eCPPTv2) w zakresie testowania i weryfikacji poprawności wdrażanych rozwiązań.

Ocena spełnienia warunków udziału w postępowaniu dokonywana będzie w oparciu o dokumenty złożone przez Wykonawcę w niniejszym postępowaniu metodą warunku granicznego - ***spełnia/nie spełnia.***

XXI. INFORMACJA O PODMIOTOWYCH ŚRODKACH DOWODOWYCH.

1. Do oferty (formularza ofertowego - wypełnionego i podpisanego przez Wykonawcę) wykonawca dołącza aktualne na dzień składania ofert **oświadczenie** o niepodleganiu wykluczeniu oraz **oświadczenie** o spełnianiu warunków udziału w postępowaniu w zakresie wskazanym przez zamawiającego.
2. Oświadczenie wykonawcy, w zakresie art. 108 ust. 1 pkt 5) ustawy, o braku przynależności do tej samej grupy kapitałowej w rozumieniu ustawy z dnia 16

lutego 2007 r. o ochronie konkurencji i konsumentów (t. j. Dz. U. z 2020 r. poz. 1076 i 1086), z innym wykonawcą, który złożył odrębną ofertę, ofertę częściową lub wniosek o dopuszczenie do udziału w postępowaniu, albo oświadczenia o przynależności do tej samej grupy kapitałowej wraz z dokumentami lub informacjami potwierdzającymi przygotowanie oferty, oferty częściowej w postępowaniu niezależnie od innego wykonawcy należącego do tej samej grupy kapitałowej.

3. Oświadczenie wykonawcy dotyczące przesłanek wykluczenia z art. 7 ust. 1 ustawy o szczególnych rozwiązaniach w zakresie przeciwdziałania wspieraniu agresji na Ukrainę oraz służących ochronie bezpieczeństwa narodowego.
4. Podmiotowe środki dowodowe oraz inne dokumenty lub oświadczenia, o których mowa w rozporządzeniu, składa się w formie elektronicznej, w postaci elektronicznej opatrzonej podpisem zaufanym lub podpisem osobistym, w formie pisemnej lub w formie dokumentowej, w zakresie i w sposób określony w przepisach wydanych na podstawie art. 70 Pzp.
5. Zgodnie z art. 139 Pzp Zamawiający najpierw dokona badania i oceny ofert, a następnie dokona kwalifikacji podmiotowej wykonawcy, którego oferta została najwyżej oceniona, w zakresie braku podstaw wykluczenia oraz spełniania warunków udziału w postępowaniu.
6. Wykonawca nie jest obowiązany do złożenia wraz z ofertą oświadczenia, o którym mowa w ust. 1, zamawiający zażąda tego oświadczenia wyłącznie od wykonawcy, którego oferta została najwyżej oceniona.

Wykonawca jest zobowiązany do wypełnienia obowiązku informacyjnego przewidzianego w art. 13 lub art. 14 RODO wobec osób fizycznych, od których dane osobowe bezpośrednio lub pośrednio pozyskał (w przypadku korzystania z podwykonawców/ podmiotów trzecich/wykonawców wchodzących w skład konsorcjum) w celu ubiegania się o udzielenie zamówienia publicznego w niniejszym postępowaniu.

XXII. PODWYKONAWCY.

1. Wykonawca, który polega na zdolnościach lub sytuacji podmiotów udostępniających zasoby, składa, wraz z wnioskiem o dopuszczenie do udziału w postępowaniu albo odpowiednio wraz z ofertą, zobowiązanie podmiotu trzeciego do oddania do dyspozycji niezbędnych zasobów na potrzeby realizacji danego zamówienia lub inny podmiotowy środek dowodowy potwierdzający, że wykonawca realizując zamówienie, będzie dysponował niezbędnymi zasobami tych podmiotów.
2. Zobowiązanie podmiotu udostępniającego zasoby potwierdza, że stosunek łączący wykonawcę z podmiotami udostępniającymi zasoby gwarantuje rzeczywisty dostęp do tych zasobów oraz określa w szczególności:
   - zakres dostępnych wykonawcy zasobów podmiotu udostępniającego zasoby;
   - sposób i okres udostępnienia wykonawcy i wykorzystania przez niego zasobów podmiotu udostępniającego te zasoby przy wykonywaniu zamówienia;
   - czy i w jakim zakresie podmiot udostępniający zasoby, na zdolnościach którego wykonawca polega w odniesieniu do warunków udziału w postępowaniu dotyczących

wykształcenia, kwalifikacji zawodowych lub doświadczenia, zrealizuje dostawy lub usługi, których wskazane zdolności dotyczą.

3. Podwykonawcy obowiązani są do złożenia wszelkich oświadczeń, w szczególności oświadczeń sankcyjnych i o braku przesłanek wykluczenia w takim zakresie w jakim dotyczą one Wykonawcy.

XXIII. WYMAGANIA ZAMAWIAJĄCEGO ZAWARTE W SWZ.

1. Zamawiający nie dopuszcza możliwości składania ofert częściowych.
2. Zamawiający nie przewiduje zawarcia umowy ramowej.
3. Zamawiający nie dopuszcza możliwości składania ofert wariantowych.
4. Zamawiający nie przewiduje rozliczenia w walutach obcych.
5. Zamawiający nie przewiduje aukcji elektronicznej.
6. Zamawiający nie przewiduje zwrotu kosztów udziału w postępowaniu.
7. Zamawiający żąda wskazania przez Wykonawcę w ofercie części zamówienia, której wykonanie zamierza powierzyć podwykonawcom z podaniem nazwy firmy.
8. Zamawiający nie ogranicza udziału Podwykonawców przy realizacji przedmiotowego zadania.

XXIV. WYMAGANIA DOTYCZĄCE WADIUM.

1. Zamawiający nie żąda od wykonawców wniesienia wadium.

XXV. INFORMACJA DOTYCZĄCA ZABEZPIECZENIE NALEŻYTEGO WYKONANIA UMOWY.

1. Zamawiający nie wymaga wniesienia zabezpieczenia należytego wykonania umowy.

XXVI. POSTANOWIENIA KOŃCOWE.

1. Protokół postępowania jest jawny i udostępniany na wniosek.
2. Załączniki do protokołu postępowania udostępnia się po dokonaniu wyboru najkorzystniejszej oferty albo unieważnieniu postępowania, z tym że:
   a) oferty wraz z załącznikami udostępnia się niezwłocznie po otwarciu ofert, nie później jednak niż w terminie 3 dni od dnia otwarcia ofert, z uwzględnieniem art. 166 ust. 3 Pzp lub art. 291 ust. 2 zdanie drugie Pzp,
3. W przypadku gdy wniesienie żądania dotyczącego prawa, o którym mowa w art. 18 ust. 1 rozporządzenia 2016/679, spowoduje ograniczenie przetwarzania danych osobowych zawartych w protokole postępowania lub załącznikach do tego protokołu, od dnia zakończenia postępowania o udzielenie zamówienia zamawiający nie udostępnia tych danych, chyba że zachodzą przesłanki, o których mowa w art. 18 ust. 2 rozporządzenia 2016/679.
4. Udostępnianie, o którym mowa w ust. 1 i 2, ma zastosowanie do wszystkich danych osobowych, z wyjątkiem danych, o których mowa w art. 9 ust. 1 rozporządzenia 2016/679, zebranych w toku postępowania o udzielenie zamówienia. Ograniczenia zasady jawności, o których mowa w ust. 3 i art. 18 ust. 3-6, stosuje się odpowiednio.

5. W sprawach nieuregulowanych zastosowanie mają przepisy ustawy Pzp.

XXVII. ZAŁĄCZNIKI.

1. Załączniki składające się na integralną cześć specyfikacji (załączniki do SWZ);
   1) formularz oferty – załącznik nr 1;
   2) opis przedmiotu zamówienia - załącznik nr 2;
   3) oświadczenie dotyczące spełniania warunków udziału w postępowaniu - załącznik nr 3;
   4) oświadczenie dotyczące przesłanek wykluczenia z postępowania – załącznik nr 4;
   5) oświadczenie dotyczące przynależności lub braku przynależności do tej samej grupy kapitałowej – załącznik nr 5;
   6) zobowiązanie podmiotu trzeciego - załącznik nr 5;
   7) oświadczenie składane na podstawie art. 117 ust. 4 ustawy Prawo zamówień publicznych - załącznik nr 7;
   8) oświadczenie wykonawcy dotyczące przesłanek wykluczenia z art. 7 ust. 1 ustawy o szczególnych rozwiązaniach w zakresie przeciwdziałania wspieraniu agresji na Ukrainę oraz służących ochronie bezpieczeństwa narodowego - załącznik nr 8;
   9) opis przedmiotu zamówienia - załącznik nr 9;
   10) wzór umowy - załącznik nr 10.

I-I.271.11.2024 Gorzyce, 15.07.2024 r.

Załącznik nr 1.

FORMULARZ OFERTOWY WYKONAWCY

Dane dotyczące zamawiającego
Gmina Gorzyce
Sandomierska 75
39-432 Gorzyce

I. Dane dotyczące wykonawcy:
Nazwa: .....
Siedziba: .....
Adres poczty elektronicznej: .....
Strona internetowa: .....
Numer telefonu: .....
Numer faksu: .....
Numer REGON: .....
Numer NIP: .....
Osoba upoważniona do reprezentacji
Wykonawcy i podpisania umowy: .....
Oświadczamy, że jesteśmy[2]:
☐ mikroprzedsiębiorstwem
☐ małym przedsiębiorstwem
☐ średnim przedsiębiorstwo
☐ dużym przedsiębiorstwem
☐ jednoosobową działalnością gospodarczą
☐ osobą fizyczną nieprowadzącą działalności gospodarczej
☐ inny rodzaj .....(podać jaki)

II. Zobowiązania wykonawcy:
Nawiązując do ogłoszenia o zamówieniu publicznym na: *Zakup sprzętu informatycznego, oprogramowania wraz ze szkoleniami i audytami w ramach konkursu grantowego Cyberbezpieczny Samorząd,* oferujemy wykonanie zamówienia zgodnie z wymogami Specyfikacji Warunków Zamówienia za cenę:

Cena netto w zł	Podatek VAT w zł	Cena brutto w zł

[2] Niepotrzebne skreślić.

I-I.271.11.2024 Gorzyce, 15.07.2024 r.

w tym:

Lp.	Nazwa elementu	Cena netto 1 szt.	VAT	Cena brutto 1 szt.	Ilość	Suma
1.	Serwer				1 szt.	
2.	Serwer				1 szt.	
3.	Serwer do wykonywania kopii zapasowych				1 szt.	
4.	Network Attached Storage (NAS)				1 szt.	
5.	Dyski twarde do macierzy dyskowej				4 szt.	
6.	Zarządzanie urządzenia sieciowe z obsługą VLAN				1 szt.	
7.	UTM				2 szt.	
8.	Macierz dyskowa				1 szt.	
9.	UPS				1 szt.	
10.	Oprogramowanie serwera				4 szt.	
11.	Licencje dostępowe				40 szt.	
12.	Oprogramowanie do wykonywania kopii zapasowych				5 szt.	
13.	Usługa w chmurze obliczeniowej typu IaaS, SaaS, PaaS dotycząca bezpieczeństwa sieciowego				1 szt.	
14.	Oprogramowanie do zarządzania i aktualizacji systemów				45 szt.	

	operacyjnych i oprogramowania na stacjach roboczych, serwerach, urządzeniach sieciowych					
15.	Oprogramowanie przeciwdziałające wyciekowi danych				45 szt.	
16.	Wdrożenie systemów teleinformatycznych				1 szt.	
17.	Wdrożenie systemów teleinformatycznych				1 szt.	
18.	Wdrożenie oprogramowania do wykonywania kopii zapasowych				1 szt.	
19.	Wdrożenie systemów teleinformatycznych				1 szt.	
20.	Wdrożenie SIEM				1 szt.	
21.	Wdrożenie oprogramowania przeciwdziałającemu wyciekowi				1 szt.	
22.	Utrzymanie systemów teleinformatycznych				1 szt.	
23.	Utrzymanie stałego wsparcia technicznego i organizacyjnego w zakresie utrzymania i doskonalenia wdrożonych standardów bezpieczeństwa				1 szt.	
24.	Wdrożenie i szkolenie				1 szt.	

	z oprogramowania do zarządzania i aktualizacji systemów operacyjnych na stacjach roboczych, serwerach, urządzeniach sieciowych oraz monitorowania infrastruktury informatycznej.					
25.	Testy penetracyjne				1 szt.	
26.	Szkolenia powiązane z testami socjotechnicznym				1 szt.	
27.	Szkolenie z cyberbezpieczeństwa dla kadry administracyjnej				1 szt.	
28.	Szkolenie z cyberbezpieczeństwa dla kadry informatycznej				1 szt.	
29.	Szkolenie specjalistyczne dla kadry zarządzającej				1 szt.	
30.	Szkolenie z oprogramowania przeciwdziałającemu wyciekowi danych				1 szt.	
31.	Szkolenie AD / wirtualizacja / kopie zapasowe				1 szt.	
32.	Opracowanie i wdrożenie dokumentacji SZBI dla Urzędu oraz Ośrodka pomocy społecznej.				1 szt.	

I-I.271.11.2024 Gorzyce, 15.07.2024 r.

Stawka podatku VAT……..%, została naliczona w oparciu o (podać podstawę prawną zastosowanej stawki podatku VAT): ……..

Czy złożenie oferty będzie skutkowało wystąpienie obowiązku odwrotnego obciążenia u Zamawiającego w myśl przepisów ustawy z dnia 11 marca 2004 r. o podatku od towarów i usług (t. j. Dz. U. 2021, poz. 685):

☐ nie,

☐ tak, w jakim zakresie …….

Oświadczam, że:

☐ Przyjmuję możliwość wykonania zamówienia poza godzinami pracy urzędu, także w soboty i niedziele.

Termin wykonania: Zamówienie będzie wykonane w miejscu siedziby zamawiającego. Dostawy sprzętu będą realizowane w ciągu 7 dni, wdrożenia w ciągu 90 dni, szkolenia w ciągu 90 dni, audyty w ciągu 90 dni.

Oświadczenie dotyczące postanowień specyfikacji warunków zamówienia:

1) Oświadczam, że zapoznałem się ze specyfikacją warunków zamówienia, nie wnoszę żadnych zastrzeżeń oraz uzyskałem niezbędne informacje do przygotowania oferty.
2) Oświadczam, że uważam się za związanego ofertą przez czas wskazany w specyfikacji warunków zamówienia.
3) Oświadczam, że załączony do specyfikacji warunków zamówienia wzór umowy zostały przeze mnie zaakceptowane bez zastrzeżeń i zobowiązuję się w przypadku wyboru mojej oferty do zawarcia umowy w miejscu i terminie wyznaczonym przez zamawiającego.

Rachunek bankowy na który będzie płatne wynagrodzenie Wykonawcy w przypadku wyboru oferty jako najkorzystniejszej:

……

……

(data i czytelny podpis wykonawcy)

I-I.271.11.2024 Gorzyce, 15.07.2024 r.

Załącznik nr 2.

OPIS PRZEDMIOTU ZAMÓWIENIA

Określone poniżej parametry są parametrami minimalnymi. Zamawiający dopuszcza sprzęt o parametrach lepszych od wymaganych pod warunkiem spełnienia wszystkich warunków minimalnych. Zamawiający wymaga, by dostarczone urządzenia były nowe (tzn. wyprodukowane w 2024 r.) oraz by nie były używane.

Zamawiający dopuszcza, by urządzenia zostały rozpakowane i uruchomione przed ich dostarczeniem wyłącznie przez Wykonawcę i wyłącznie w celu weryfikacji działania urządzenia.

1. **Serwer – 1 sztuka.**

Parametr	Charakterystyka (wymagania minimalne)
Obudowa	• Obudowa Rack o wysokości max 2U wraz z kompletem wysuwanych szyn umożliwiających montaż w szafie rack i wysuwanie serwera do celów serwisowych. • Obudowa z możliwością wyposażenia w panel LCD umieszczony na froncie obudowy, umożliwiający wyświetlenie informacji o stanie procesora, pamięci, dysków, BIOS'u, zasilaniu oraz temperaturze. • Obudowa z możliwością wyposażenia 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	• Płyta główna z możliwością zainstalowania do dwóch procesorów. • Obsługa procesorów 32 rdzeniowych. • Płyta główna musi być zaprojektowana przez producenta serwera i oznaczona jego znakiem firmowym. • Na płycie głównej powinno znajdować się minimum 16 sloty przeznaczone do instalacji pamięci. • Płyta główna powinna obsługiwać do 1TB pamięci RAM.
Chipset	• Dedykowany przez producenta procesora do pracy w serwerach dwuprocesorowych
Procesor	• Zainstalowany jeden procesor min. 16-rdzeniowy klasy x86, min. 2.0GHz, dedykowany do pracy z zaoferowanym serwerem umożliwiający osiągnięcie wyniku min. 265 w teście SPECrate2017_int_base, dostępnym na stronie www.spec.org dla konfiguracji dwuprocesorowej.

I-I.271.11.2024 Gorzyce, 15.07.2024 r.

RAM	• Minimum 256GB DDR5 RDIMM 4800MT/s,
Funkcjonalność pamięci RAM	• Demand Scrubbing, • Patrol Scrubbing, • Permanent Fault Detection (PFD)
Gniazda PCI	• Min. dwa sloty PCIe
Interfejsy sieciowe/FC/SAS	• Wbudowane min. 2 interfejsy sieciowe 1Gb Ethernet w standardzie BaseT • Dodatkowa karta Dual Port (2x SFP+, 10Gb/s, SFP+, PCIe) • Dodatkowa karta SAS (4x mini SAS-HD, 12Gb/s, SAS, PCIe)
Dyski twarde	• Zainstalowane dwa dyski M.2 NVME o pojemności min. 480GB Hot-Plug z możliwością konfiguracji RAID 1.
Wbudowane porty	• 4x USB, w tym min. 1 porty USB 3.0 • 2x port VGA (jeden na panelu przednim) • Możliwość rozbudowy o Serial Port
Video	• Zintegrowana karta graficzna umożliwiająca wyświetlenie rozdzielczości min. 1280x1024
Wentylatory	• Redundantne, Hot-Plug
Zasilacze	• Redundantne, Hot-Plug min. 1100W klasy Titanium
Bezpieczeństwo	• Zatrzask górnej pokrywy oraz blokada na ramce panela zamykana na klucz służąca do ochrony nieautoryzowanego dostępu do dysków twardych. • Możliwość wyłączenia w BIOS funkcji przycisku zasilania. • BIOS ma możliwość przejścia do bezpiecznego trybu rozruchowego z możliwością zarządzania blokadą zasilania, panelem sterowania oraz zmianą hasła

I-I.271.11.2024 Gorzyce, 15.07.2024 r.

	• Wbudowany czujnik otwarcia obudowy współpracujący z BIOS i kartą zarządzającą. • Moduł TPM 2.0 • Możliwość dynamicznego włączania I wyłączania portów USB na obudowie – bez potrzeby restartu serwera • Możliwość wymazania danych ze znajdujących się dysków wewnątrz serwera – niezależne od zainstalowanego systemu operacyjnego, uruchamiane z poziomu zarządzania serwerem • Serwer musi być wyposażony w rozwiązanie zapewniające ochronę oprogramowania układowego przed manipulacją złośliwego oprogramowania. Ochrona taka musi być zgodna z zaleceniami NIST SP 800-147B i NIST SP 800-155. Jednocześnie Zamawiający wymaga, aby dostarczony serwer posiadał zaimplementowane sprzętowo mechanizmy kryptograficzne poświadczające integralność oprogramowania BIOS (Root of Trust).
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 autentykacje 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; ○ integracja z Active Directory; ○ możliwość obsługi 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 oraz z możliwością rozszerzenia funkcjonalności o: ○ Wirtualny schowek ułatwiający korzystanie z konsoli zdalnej ○ Przesyłanie danych telemetrycznych w czasie rzeczywistym ○ Dostosowanie zarządzania temperaturą i przepływem powietrza w serwerze ○ Automatyczna rejestracja certyfikatów (ACE)

I-I.271.11.2024 Gorzyce, 15.07.2024 r.

Oprogramowanie do zarządzania	• Możliwość zainstalowania oprogramowania producenta do zarządzania, spełniającego poniższe wymagania: o Wsparcie dla serwerów, urządzeń sieciowych oraz pamięci masowych o integracja z Active Directory o Możliwość zarządzania dostarczonymi serwerami bez udziału dedykowanego agenta o Wsparcie dla protokołów SNMP, IPMI, Linux SSH, Redfish o Możliwość uruchamiania procesu wykrywania urządzeń w oparciu o harmonogram o Szczegółowy opis wykrytych systemów oraz ich komponentów o Możliwość eksportu raportu do CSV, HTML, XLS, PDF o Możliwość tworzenia własnych raportów w oparciu o wszystkie informacje zawarte w inwentarzu. o Grupowanie urządzeń w oparciu o kryteria użytkownika o Tworzenie automatycznie grup urządzeń w oparciu o dowolny element konfiguracji serwera np. Nazwa, lokalizacja, system operacyjny, obsadzenie slotów PCIe, pozostałego czasu gwarancji o Możliwość uruchamiania narzędzi zarządzających w poszczególnych urządzeniach o Szybki podgląd stanu środowiska o Podsumowanie stanu dla każdego urządzenia o Szczegółowy status urządzenia/elementu/komponentu o Generowanie alertów przy zmianie stanu urządzenia. o Filtry raportów umożliwiające podgląd najważniejszych zdarzeń o Integracja z service desk producenta dostarczonej platformy sprzętowej o Możliwość przejęcia zdalnego pulpitu o Możliwość podmontowania wirtualnego napędu o Kreator umożliwiający dostosowanie akcji dla wybranych alertów o Możliwość importu plików MIB o Przesyłanie alertów „as-is” do innych konsol firm trzecich o Możliwość definiowania ról administratorów o Możliwość zdalnej aktualizacji oprogramowania wewnętrznego serwerów o Aktualizacja oparta o wybranie źródła bibliotek (lokalna, on-line producenta oferowanego rozwiązania) o Możliwość instalacji oprogramowania wewnętrznego bez potrzeby instalacji agenta o Możliwość automatycznego generowania i zgłaszania incydentów awarii bezpośrednio do centrum serwisowego producenta serwerów o Moduł raportujący pozwalający na wygenerowanie następujących informacji: nr seryjne sprzętu, konfiguracja poszczególnych urządzeń, wersje oprogramowania wewnętrznego, obsadzenie slotów PCI i gniazd pamięci, informację o maszynach wirtualnych, aktualne informacje o stanie i poziomie gwarancji, adresy IP kart sieciowych, występujących alertów, MAC adresów kart sieciowych, stanie poszczególnych komponentów serwera. o Możliwość tworzenia sprzętowej konfiguracji bazowej i na jej podstawie weryfikacji środowiska w celu wykrycia rozbieżności. o Wdrażanie serwerów, rozwiązań modularnych oraz przełączników sieciowych w oparciu o profile

I-I.271.11.2024 Gorzyce, 15.07.2024 r.

	○ Możliwość migracji ustawień serwera wraz z wirtualnymi adresami sieciowymi (MAC, WWN, IQN) między urządzeniami. ○ Tworzenie gotowych paczek informacji umożliwiających zdiagnozowanie awarii urządzenia przez serwis producenta. ○ Zdalne uruchamianie diagnostyki serwera. ○ Dedykowana aplikacja na urządzenia mobilne integrująca się z wyżej opisanymi oprogramowaniem zarządzającym. ○ Oprogramowanie dostarczane jako wirtualny appliance dla KVM, ESXi i Hyper-V.
Certyfikaty	• Serwer musi być wyprodukowany zgodnie z normą ISO-9001:2015, ISO-50001 oraz ISO-14001 • Serwer musi posiadać deklaracja CE. • Serwer musi spełniać wymagania normy NIST SP 800-193 ochrony przed cyberatakami. • Oferowane produkty muszą 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 jest wydruk ze strony internetowej www.epeat.net potwierdzający spełnienie normy co najmniej Epeat Silver według normy wprowadzonej w 2019 roku - **Wykonawca złoży dokument potwierdzający spełnianie wymogu.** • Oferowany serwer musi znajdować się na liście Windows Server Catalog i posiadać status „Certified for Windows" dla systemów Microsoft Windows Server 2019, Microsoft Windows Server 2022.
Dokumentacja użytkownika	• Zamawiający wymaga dokumentacji w języku polskim lub angielskim. • Możliwość telefonicznego sprawdzenia konfiguracji sprzętowej serwera oraz warunków gwarancji po podaniu numeru seryjnego bezpośrednio u producenta lub jego przedstawiciela.
Warunki gwarancji	• Zamawiający wymaga zapewnienia gwarancji Producenta z zakresu wdrażanej technologii na okres 5 lat. • Zamawiający oczekuje możliwości zgłaszania zdarzeń serwisowych w trybie 24/7/365 następującymi kanałami: telefonicznie, przez Internet oraz z wykorzystaniem aplikacji. • Zamawiający oczekuje bezpośredniego dostępu do wykwalifikowanej kadry inżynierów technicznych a w przypadku konieczności eskalacji zgłoszenia serwisowego wyznaczonego Kierownika Eskalacji po stronie Producenta (dla krytycznych zgłoszeń serwisowych) • Zamawiający wymaga pojedynczego punktu kontaktu dla całego rozwiązania Producenta, w tym także sprzedanego oprogramowania. • Zgłoszenie przyjęte jest potwierdzane przez zespół pomocy technicznej (mail/telefon / aplikacja / portal) przez nadanie unikalnego numeru zgłoszenia

	pozwalającego na identyfikację zgłoszenia w trakcie realizacji naprawy i po jej zakończeniu.
	• Zamawiający oczekuje możliwości samodzielnego kwalifikowania poziomu ważności naprawy.
	• Zamawiający oczekuje rozpoczęcia diagnostyki telefonicznej / internetowej już w momencie dokonania zgłoszenia. Certyfikowany Technik Producenta z właściwym zestawem części do naprawy (potwierdzonym na etapie diagnostyki) powinien rozpocząć naprawę w siedzibie zamawiającego najpóźniej w następnym dniu roboczym (NBD) od otrzymania zgłoszenia / zakończenia diagnostyki. Naprawa ma się odbyć w siedzibie zamawiającego, chyba, że zamawiający dla danej naprawy zgodzi się na inną formę.
	• Zamawiający oczekuje nieodpłatnego udostępnienia narzędzi serwisowych i procesów wsparcia umożliwiających: Wykrywanie usterek sprzętowych z predykcją awarii, automatyczną diagnostykę i zdalne otwieranie zgłoszeń serwisowych, wskazówki dotyczące bezpieczeństwa produktów, samodzielne wysyłanie części, a także ocena bezpieczeństwa cybernetycznego.
	• Zamawiający wymaga od podmiotu realizującego serwis lub producenta sprzętu dołączenia do oferty oświadczenia, że w przypadku wystąpienia awarii dysku twardego w urządzeniu objętym aktywnym wparciem technicznym, uszkodzony dysk twardy pozostaje u Zamawiającego.
	• Możliwość rozszerzenia gwarancji Producenta o usługę diagnostyki sprzętu na miejscu w przypadku awarii. Charakterystyka usługi diagnostyki:
	  ○ Możliwości utworzenia zgłaszania serwisowego w wyniku, którego proces diagnostyki odbędzie się na miejscu w siedzibie zamawiającego.
	  ○ Po przyjeździe do siedziby Zamawiającego, pracownik serwisu przystąpi do rozwiązywania problemu. Jeśli do rozwiązania problemu będzie konieczna dodatkowa pomoc diagnostyczna lub części, pracownik serwisu może w imieniu Zamawiającego skontaktować się z producentem w celu uzyskania pomocy.
	  ○ Reakcja na miejscu u Zamawiającego powinna nastąpić w okresie zgodnym z czasem reakcji przypisanym do urządzenia, które posiada wykupioną usługę serwisową.
	  ○ Pracownik serwisu powinien skontaktować się z Zamawiającym przed przyjazdem na miejsce w celu sprawdzenia zgłoszenia, ustalenia harmonogramu i potwierdzenia wszelkich informacji niezbędnych do realizacji wizyty technika na miejscu.
	  ○ Jeśli w trakcie wstępnego procesu rozwiązywania problemu na miejscu awarii zostanie ustalone, że do realizacji usługi jest niezbędna jakaś część, znajdujący się na miejscu pracownik serwisu zamówi nową część i przekaże dodatkowe zgłoszenie do działu obsługi technicznej. Technik pracujący na miejscu powróci do siedziby Klienta w celu wymiany wysłanej części w ciągu czasu reakcji ustalonego zgodnie z umową serwisową zakupionego produktu.
	• Wymagane dołączenie do oferty oświadczenia Producenta potwierdzające, że Serwis urządzeń będzie realizowany bezpośrednio przez Producenta i/lub we współpracy z Autoryzowanym Partnerem Serwisowym Producenta.
	• Firma serwisująca musi posiadać ISO 9001:2015 oraz ISO-27001 na świadczenie usług serwisowych oraz posiadać autoryzacje producenta urządzeń – dokumenty potwierdzające należy załączyć do oferty.

I-I.271.11.2024 Gorzyce, 15.07.2024 r.

2. Serwer – 1 sztuka.

Parametr	Charakterystyka (wymagania minimalne)
Obudowa	• Obudowa Rack o wysokości max 2U wraz z kompletem wysuwanych szyn umożliwiających montaż w szafie rack i wysuwanie serwera do celów serwisowych. • Obudowa z możliwością wyposażenia w panel LCD umieszczony na froncie obudowy, umożliwiający wyświetlenie informacji o stanie procesora, pamięci, dysków, BIOS'u, zasilaniu oraz temperaturze. • Obudowa z możliwością wyposażenia 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	• Płyta główna z możliwością zainstalowania do dwóch procesorów. • Obsługa procesorów 32 rdzeniowych. • Płyta główna musi być zaprojektowana przez producenta serwera i oznaczona jego znakiem firmowym. • Na płycie głównej powinno znajdować się minimum 16 sloty przeznaczone do instalacji pamięci. • Płyta główna powinna obsługiwać do 1TB pamięci RAM.
Chipset	• Dedykowany przez producenta procesora do pracy w serwerach dwuprocesorowych
Procesor	• Zainstalowany jeden procesor min. 16-rdzeniowy klasy x86, min. 2.0GHz, dedykowany do pracy z zaoferowanym serwerem umożliwiający osiągnięcie wyniku min. 265 w teście SPECrate2017_int_base, dostępnym na stronie www.spec.org dla konfiguracji dwuprocesorowej.
RAM	• Minimum 256GB DDR5 RDIMM 4800MT/s,
Funkcjonalność pamięci RAM	• Demand Scrubbing, • Patrol Scrubbing, • Permanent Fault Detection (PFD)
Gniazda PCI	• Min. dwa sloty PCIe

I-I.271.11.2024 Gorzyce, 15.07.2024 r.

Interfejsy sieciowe/FC/SAS	• Wbudowane min. 2 interfejsy sieciowe 1Gb Ethernet w standardzie BaseT • Dodatkowa karta Dual Port (2x SFP+, 10Gb/s, SFP+, PCIe)
Dyski twarde	• Zainstalowane dwa dyski M.2 NVME o pojemności min. 480GB Hot-Plug z możliwością konfiguracji RAID 1.
Wbudowane porty	• 4x USB, w tym min. 1 porty USB 3.0 • 2x port VGA (jeden na panelu przednim) • Możliwość rozbudowy o Serial Port
Video	• Zintegrowana karta graficzna umożliwiająca wyświetlenie rozdzielczości min. 1280x1024
Wentylatory	• Redundantne, Hot-Plug
Zasilacze	• Redundantne, Hot-Plug min. 1100W klasy Titanium
Bezpieczeństwo	• Zatrzask górnej pokrywy oraz blokada na ramce panela zamykana na klucz służąca do ochrony nieautoryzowanego dostępu do dysków twardych. • Możliwość wyłączenia w BIOS funkcji przycisku zasilania. • BIOS ma możliwość przejścia do bezpiecznego trybu rozruchowego z możliwością zarządzania blokadą zasilania, panelem sterowania oraz zmianą hasła • Wbudowany czujnik otwarcia obudowy współpracujący z BIOS i kartą zarządzającą. • Moduł TPM 2.0 • Możliwość dynamicznego włączania I wyłączania portów USB na obudowie – bez potrzeby restartu serwera • Możliwość wymazania danych ze znajdujących się dysków wewnątrz serwera – niezależne od zainstalowanego systemu operacyjnego, uruchamiane z poziomu zarządzania serwerem • Serwer musi być wyposażony w rozwiązanie zapewniające ochronę oprogramowania układowego przed manipulacją złośliwego oprogramowania. Ochrona taka musi być zgodna z zaleceniami NIST SP 800-147B i NIST SP 800-155. Jednocześnie Zamawiający wymaga, aby dostarczony serwer posiadał zaimplementowane sprzętowo mechanizmy kryptograficzne poświadczające integralność oprogramowania BIOS (Root of Trust).

I-I.271.11.2024 Gorzyce, 15.07.2024 r.

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 autentykacje 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; ○ integracja z Active Directory; ○ możliwość obsługi 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 oraz z możliwością rozszerzenia funkcjonalności o: ○ Wirtualny schowek ułatwiający korzystanie z konsoli zdalnej ○ Przesyłanie danych telemetrycznych w czasie rzeczywistym ○ Dostosowanie zarządzania temperaturą i przepływem powietrza w serwerze ○ Automatyczna rejestracja certyfikatów (ACE)
Oprogramowanie do zarządzania	• Możliwość zainstalowania oprogramowania producenta do zarządzania, spełniającego poniższe wymagania: ○ Wsparcie dla serwerów, urządzeń sieciowych oraz pamięci masowych ○ integracja z Active Directory ○ Możliwość zarządzania dostarczonymi serwerami bez udziału dedykowanego agenta ○ Wsparcie dla protokołów SNMP, IPMI, Linux SSH, Redfish ○ Możliwość uruchamiania procesu wykrywania urządzeń w oparciu o harmonogram ○ Szczegółowy opis wykrytych systemów oraz ich komponentów ○ Możliwość eksportu raportu do CSV, HTML, XLS, PDF ○ Możliwość tworzenia własnych raportów w oparciu o wszystkie informacje zawarte w inwentarzu. ○ Grupowanie urządzeń w oparciu o kryteria użytkownika ○ Tworzenie automatycznie grup urządzeń w oparciu o dowolny element konfiguracji serwera np. Nazwa, lokalizacja, system operacyjny, obsadzenie slotów PCIe, pozostałego czasu gwarancji ○ Możliwość uruchamiania narzędzi zarządzających w poszczególnych urządzeniach ○ Szybki podgląd stanu środowiska

	○ Podsumowanie stanu dla każdego urządzenia ○ Szczegółowy status urządzenia/elementu/komponentu ○ Generowanie alertów przy zmianie stanu urządzenia. ○ Filtry raportów umożliwiające podgląd najważniejszych zdarzeń ○ Integracja z service desk producenta dostarczonej platformy sprzętowej ○ Możliwość przejęcia zdalnego pulpitu ○ Możliwość podmontowania wirtualnego napędu ○ Kreator umożliwiający dostosowanie akcji dla wybranych alertów ○ Możliwość importu plików MIB ○ Przesyłanie alertów „as-is" do innych konsol firm trzecich ○ Możliwość definiowania ról administratorów ○ Możliwość zdalnej aktualizacji oprogramowania wewnętrznego serwerów ○ Aktualizacja oparta o wybranie źródła bibliotek (lokalna, on-line producenta oferowanego rozwiązania) ○ Możliwość instalacji oprogramowania wewnętrznego bez potrzeby instalacji agenta ○ Możliwość automatycznego generowania i zgłaszania incydentów awarii bezpośrednio do centrum serwisowego producenta serwerów ○ Moduł raportujący pozwalający na wygenerowanie następujących informacji: nr seryjne sprzętu, konfiguracja poszczególnych urządzeń, wersje oprogramowania wewnętrznego, obsadzenie slotów PCI i gniazd pamięci, informację o maszynach wirtualnych, aktualne informacje o stanie i poziomie gwarancji, adresy IP kart sieciowych, występujących alertów, MAC adresów kart sieciowych, stanie poszczególnych komponentów serwera. ○ Możliwość tworzenia sprzętowej konfiguracji bazowej i na jej podstawie weryfikacji środowiska w celu wykrycia rozbieżności. ○ Wdrażanie serwerów, rozwiązań modularnych oraz przełączników sieciowych w oparciu o profile ○ Możliwość migracji ustawień serwera wraz z wirtualnymi adresami sieciowymi (MAC, WWN, IQN) między urządzeniami. ○ Tworzenie gotowych paczek informacji umożliwiających zdiagnozowanie awarii urządzenia przez serwis producenta. ○ Zdalne uruchamianie diagnostyki serwera. ○ Dedykowana aplikacja na urządzenia mobilne integrująca się z wyżej opisanymi oprogramowaniem zarządzającym. ○ Oprogramowanie dostarczane jako wirtualny appliance dla KVM, ESXi i Hyper-V.
Certyfikaty	• Serwer musi być wyprodukowany zgodnie z normą ISO-9001:2015, ISO-50001 oraz ISO-14001 • Serwer musi posiadać deklaracja CE. • Serwer musi spełniać wymagania normy NIST SP 800-193 ochrony przed cyberatakami. • Oferowane produkty muszą 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-I.271.11.2024 Gorzyce, 15.07.2024 r.

	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 jest wydruk ze strony internetowej www.epeat.net potwierdzający spełnienie normy co najmniej Epeat Silver według normy wprowadzonej w 2019 roku - **Wykonawca złoży dokument potwierdzający spełnianie wymogu.** • Oferowany serwer musi znajdować się na liście Windows Server Catalog i posiadać status „Certified for Windows" dla systemów Microsoft Windows Server 2019, Microsoft Windows Server 2022.
Dokumentacja użytkownika	• Zamawiający wymaga dokumentacji w języku polskim lub angielskim. • Możliwość telefonicznego sprawdzenia konfiguracji sprzętowej serwera oraz warunków gwarancji po podaniu numeru seryjnego bezpośrednio u producenta lub jego przedstawiciela.
Warunki gwarancji	• Zamawiający wymaga zapewnienia gwarancji Producenta z zakresu wdrażanej technologii na okres 5 lat. • Zamawiający oczekuje możliwości zgłaszania zdarzeń serwisowych w trybie 24/7/365 następującymi kanałami: telefonicznie, przez Internet oraz z wykorzystaniem aplikacji. • Zamawiający oczekuje bezpośredniego dostępu do wykwalifikowanej kadry inżynierów technicznych a w przypadku konieczności eskalacji zgłoszenia serwisowego wyznaczonego Kierownika Eskalacji po stronie Producenta (dla krytycznych zgłoszeń serwisowych) • Zamawiający wymaga pojedynczego punktu kontaktu dla całego rozwiązania Producenta, w tym także sprzedanego oprogramowania. • Zgłoszenie przyjęte jest potwierdzane przez zespół pomocy technicznej (mail/telefon / aplikacja / portal) przez nadanie unikalnego numeru zgłoszenia pozwalającego na identyfikację zgłoszenia w trakcie realizacji naprawy i po jej zakończeniu. • Zamawiający oczekuje możliwości samodzielnego kwalifikowania poziomu ważności naprawy. • Zamawiający oczekuje rozpoczęcia diagnostyki telefonicznej / internetowej już w momencie dokonania zgłoszenia. Certyfikowany Technik Producenta z właściwym zestawem części do naprawy (potwierdzonym na etapie diagnostyki) powinien rozpocząć naprawę w siedzibie zamawiającego najpóźniej w następnym dniu roboczym (NBD) od otrzymania zgłoszenia / zakończenia diagnostyki. Naprawa ma się odbyć w siedzibie zamawiającego, chyba, że zamawiający dla danej naprawy zgodzi się na inną formę. • Zamawiający oczekuje nieodpłatnego udostępnienia narzędzi serwisowych i procesów wsparcia umożliwiających: Wykrywanie usterek sprzętowych z predykcją awarii, automatyczną diagnostykę i zdalne otwieranie zgłoszeń serwisowych, wskazówki dotyczące bezpieczeństwa produktów, samodzielne wysyłanie części, a także ocena bezpieczeństwa cybernetycznego. • Zamawiający wymaga od podmiotu realizującego serwis lub producenta sprzętu dołączenia do oferty oświadczenia, że w przypadku wystąpienia awarii dysku

	twardego w urządzeniu objętym aktywnym wparciem technicznym, uszkodzony dysk twardy pozostaje u Zamawiającego. • Możliwość rozszerzenia gwarancji Producenta o usługę diagnostyki sprzętu na miejscu w przypadku awarii. Charakterystyka usługi diagnostyki: ○ Możliwości utworzenia zgłaszania serwisowego w wyniku, którego proces diagnostyki odbędzie się na miejscu w siedzibie zamawiającego. ○ Po przyjeździe do siedziby Zamawiającego, pracownik serwisu przystąpi do rozwiązywania problemu. Jeśli do rozwiązania problemu będzie konieczna dodatkowa pomoc diagnostyczna lub części, pracownik serwisu może w imieniu Zamawiającego skontaktować się z producentem w celu uzyskania pomocy. ○ Reakcja na miejscu u Zamawiającego powinna nastąpić w okresie zgodnym z czasem reakcji przypisanym do urządzenia, które posiada wykupioną usługę serwisową. ○ Pracownik serwisu powinien skontaktować się z Zamawiającym przed przyjazdem na miejsce w celu sprawdzenia zgłoszenia, ustalenia harmonogramu i potwierdzenia wszelkich informacji niezbędnych do realizacji wizyty technika na miejscu. ○ Jeśli w trakcie wstępnego procesu rozwiązywania problemu na miejscu awarii zostanie ustalone, że do realizacji usługi jest niezbędna jakaś część, znajdujący się na miejscu pracownik serwisu zamówi nową część i przekaże dodatkowe zgłoszenie do działu obsługi technicznej. Technik pracujący na miejscu powróci do siedziby Klienta w celu wymiany wysłanej części w ciągu czasu reakcji ustalonego zgodnie z umową serwisową zakupionego produktu. • Wymagane dołączenie do oferty oświadczenia Producenta potwierdzające, że Serwis urządzeń będzie realizowany bezpośrednio przez Producenta i/lub we współpracy z Autoryzowanym Partnerem Serwisowym Producenta. • Firma serwisująca musi posiadać ISO 9001:2015 oraz ISO-27001 na świadczenie usług serwisowych oraz posiadać autoryzacje producenta urządzeń – dokumenty potwierdzające należy załączyć do oferty.

3. Serwer do wykonywania kopii zapasowych - 1 sztuka.

Komponent	Minimalne wymagania
Obudowa i pojemność	Wysokość maksymalnie 1U do instalacji w szafie Rack. Co najmniej 9 slotów przeznaczonych na zestaw taśm.
Połączenie	Co najmniej 1 port SAS o przepustowości co najmniej 6Gb/s w standardzie umożliwiającym podłączenie serwerów.
Napęd	Wyposażony w co najmniej 1 sztukę napędu SAS LTO8. W komplecie: • kabel SAS umożliwiający podłączenie biblioteki do serwera o dł. min. 2m • 10x taśma LTO8 WORM • Oznaczenia dla taśm LTO8, numery: 1-200

	• Oznaczenia dla taśm LTO8 WORM, numery: 1-200 • Taśma czyszcząca
Gwarancja	5 lat gwarancji producenta Zamawiający oczekuje możliwości zgłaszania zdarzeń serwisowych w trybie 24/7/365 następującymi kanałami: telefonicznie, przez Internet oraz z wykorzystaniem aplikacji. Zamawiający oczekuje rozpoczęcia diagnostyki telefonicznej / internetowej już w momencie dokonania zgłoszenia. Certyfikowany Technik wykonawcy / producenta z właściwym zestawem części do naprawy (potwierdzonym na etapie diagnostyki) ma rozpocząć naprawę w siedzibie zamawiającego najpóźniej w następnym dniu roboczym (NBD) od otrzymania zgłoszenia / zakończenia diagnostyki. Naprawa ma się odbywać w siedzibie zamawiającego, chyba, że zamawiający dla danej naprawy zgodzi się na inną formę. Zamawiający oczekuje bezpośredniego dostępu do wykwalifikowanej kadry inżynierów technicznych a w przypadku konieczności eskalacji zgłoszenia serwisowego wyznaczonego Kierownika Eskalacji po stronie wykonawcy. Zamawiający wymaga pojedynczego punktu kontaktu dla całego rozwiązania producenta, w tym także sprzedanego oprogramowania. Zgłoszenie przyjęte jest potwierdzane przez zespół pomocy technicznej (mail/telefon / aplikacja / portal) przez nadanie unikalnego numeru zgłoszenia pozwalającego na identyfikację zgłoszenia w trakcie realizacji naprawy i po jej zakończeniu. Zamawiający oczekuje możliwości samodzielnego kwalifikowania poziomu ważności naprawy. Możliwość sprawdzenia statusu gwarancji poprzez stronę producenta podając unikatowy numer urządzenia oraz pobieranie uaktualnień mikrokodu oraz sterowników nawet w przypadku wygaśnięcia gwarancji urządzenia. Automatyczną diagnostykę i zdalne otwieranie zgłoszeń serwisowych. Firma serwisująca musi posiadać ISO 9001:2015 oraz ISO-27001 na świadczenie usług serwisowych oraz posiadać autoryzacje producenta urządzeń – dokumenty potwierdzające należy załączyć do oferty. Wymagane dołączenie do oferty oświadczenia Producenta potwierdzając, że Serwis urządzeń będzie realizowany bezpośrednio przez Producenta i/lub we współpracy z Autoryzowanym Partnerem Serwisowym Producenta.

4. Network Attached Storage (NAS) - 1 sztuka.

Typ urządzenia	**Serwer NAS**
Obudowa	Tower
Procesor	Czterordzeniowy procesor o taktowaniu 2.0 GHz (maksymalnie 2,7 GHz z przyspieszeniem) osiągający w teście PassMark co najmniej 2900 punktów
Sprzętowy mechanizm szyfrowania	Tak (AES-NI)
Pamięć RAM	min. 2 GB pamięci non-ECC SODIMM z możliwością rozszerzenia do min. 6 GB

I-I.271.11.2024 Gorzyce, 15.07.2024 r.

Możliwości rozbudowy	Sprzęt powinien być wyposażony w min. 4 kieszenie na dyski twarde typu hot-swap Wbudowane 2 gniazda M.2 obsługujące dyski NVMe. Dyski NVMe mogą posłużyć do utworzenia pamięć podręcznej bądź przestrzeni dyskowej
Porty zewnętrzne	Minimum: • 2 porty USB 3.2.1
Porty sieciowe	Minimum: • 2 porty 1GbE RJ45 (z obsługą funkcji Link Aggregation / przełączania awaryjnego)
Funkcja Wake on LAN/WAN	Tak
Wentylator obudowy	Min. 2 wentylatory 92 mm x 92 mm
Obsługiwane protokoły sieciowe	Min. SMB1 (CIFS), SMB2, SMB3, NFSv3, NFSv4, NFSv4.1, NFS Kerberized sessions, iSCSI, HTTP, HTTPs, FTP, SNMP, LDAP, CalDAV
Obsługiwane systemy plików	Min.: • Wewnętrzny: Btrfs, ext4 • Zewnętrzny: Btrfs, ext4, ext3, FAT, NTFS, HFS+, exFAT
Zarządzanie pamięcią masową	• Maksymalny rozmiar pojedynczego wolumenu: 108 TB • Minimalny liczba wewnętrznych wolumenów: 64 • Minimalny liczba obiektów iSCSI Target: 128 • Minimalny liczba jednostek iSCSI LUN: 256 • Obsługa klonowania/migawek jednostek iSCSI LUN
Obsługiwane typy macierzy RAID	Synology Hybrid RAID (SHR), Podstawowy (Basic), JBOD, RAID 0, RAID 1, RAID 5, RAID 6, RAID 10
Funkcja udostępniania plików	• Minimalna liczba kont użytkowników: 2048 • Minimalna liczba grup użytkowników: 256 • Minimalna liczba folderów współdzielonych: 512 • Minimalna liczba jednoczesnych połączeń SMB/NFS/AFP/FTP: 500 • Minimalna liczba jednoczesnych połączeń protokołu SMB/AFP/FTP (z rozbudową pamięci RAM): 1500
Uprawnienia	Uprawnienia aplikacji listy kontroli dostępu systemu Windows (ACL)
Wirtualizacja	Obsługa VMware vSphere®, Citrix®, OpenStack®
Usługa katalogowa	Integracja z usługami Windows® AD Logowanie użytkowników domeny przez protokoły SMB/NFS/AFP/FTP lub aplikację File Station, integracja z LDAP
Bezpieczeństwo	Zapora, szyfrowanie folderu współdzielonego, szyfrowanie SMB, FTP przez SSL/TLS, SFTP, rsync przez SSH, automatyczne

	blokowanie logowania, obsługa Let's Encrypt, HTTPS (dostosowywane mechanizmy szyfrowania)
Obsługiwane systemy klienckie	Windows® 7 i nowsze, macOS® 10.12 i nowsze
Obsługiwane przeglądarki	Chrome®, Firefox®, Edge®, Internet Explorer® 10 i nowsze, Safari® 10 i nowsze, Safari (iOS 10 i nowsze), Chrome (Android™ 6.0 i nowsze) na tabletach
Zasilanie	Wymogiem jest dostarczenie sprzętu wyposażonego w zasilacz maks. 90 W
Oprogramowanie	• Urządzenie musi umożliwiać utworzenie przestrzeni dyskowej w oparciu o nowoczesny system plików, który będzie zapewniał obsługę migawek, generowania sum kontrolnych CRC a także lustrzanych kopii metadanych, aby zapewnić całkowitą integralność danych biznesowych. Dodatkowo wspomniany system musi wspierać ustawienie limitu dla folderów współdzielonych oraz szybkie klonowanie całych folderów udostępnionych • Oprogramowanie zarządzające serwerem NAS musi zapewnić darmowe, kompleksowe rozwiązanie do tworzenia kopii zapasowych przeznaczone dla heterogenicznych środowisk IT, umożliwiające zdalne zarządzanie i monitorowanie ochrony komputerów, serwerów i maszyn wirtualnych na jednym, centralnym, przyjaznym dla administratora interfejsie. Ponadto gromadzone dane na urządzeniu mają mieć możliwość replikacji jako lokalne kopie zapasowe, sieciowe kopie zapasowe i kopie zapasowe danych w chmurach publicznych przy użyciu darmowego narzędzia instalowanego z Centrum Pakietów • Wymaga się zapewnienia darmowej aplikacji do realizacji chmury prywatnej bez opłat cyklicznych, która będzie posiadała wygodną konsolę administratora zarządzaną z GUI a także agenty na urządzenia PC/MAC oraz aplikację mobilną na Android/iOS. Usługa powinna umożliwiać udostępnianie zasobów serwera NAS, synchronizację i tworzenie kopii zapasowych podłączonych urządzeń a także wspierać algorytm Intelliversioning. Ponadto omawiana usługa powinna umożliwiać pracę z dokumentami biurowymi (edytor tekstowy, arkusz kalkulacyjny, pokaz slajdów) i wpierać wersjonowanie oraz edycję tworzonych plików office w czasie rzeczywistym. • Urządzenie musi umożliwiać pracę w trybie klastra wysokiej dostępności (HA) aby zapewnić nieprzerwany, natychmiastowy dostęp do zasobów bez widocznych zmian w użytkowaniu (konfiguracja jako jeden spójny system). Wszystkie dane z powodzeniem zapisane na serwerze aktywnym będą na bieżąco kopiowane do serwera • pasywnego zapewniając replikację w czasie rzeczywistym i dostęp do danych oraz usług w przypadku uszkodzenia jednostki aktywnej dając gwarancję ciągłości pracy. Utworzenie klastra HA ma się opierać o 2 identyczne urządzenia.
Gwarancja	Wykonawca udzieli gwarancji: • 3 lat na urządzenia główne z możliwością przedłużenia do 5 lat za pomocą dodatkowego pakietu gwarancyjnego

I-I.271.11.2024 Gorzyce, 15.07.2024 r.

5. Dyski twarde do macierzy dyskowej - 4 sztuki.

Minimalne wymagania:	
Pojemność	min. 8000 GB
Typ	HDD (magnetyczny)
Format	Format 3,5 cala
Interfejs	Serial ATA III
Pamięć cache	min. 256 MB
Prędkość obrotowa	7200 obr./ min.

6. Zarządzanie urządzenia sieciowe z obsługą VLAN - 1 sztuka.

I. CECHY ZARZĄDZANIA		
1.	Typ przełącznika	Zarządzany
2.	Przełącznik wielowarstwowy	L2/L3
3.	Obsługa jakość serwisu (QoS)	Tak
4.	Zarządzany w chmurze	Tak
5.	Zarządzanie przez stronę www	Tak
6.	Inspekcja ARP	Tak

I-I.271.11.2024 Gorzyce, 15.07.2024 r.

7.	Konfigurowanie ustawień lokalizacji (CLI)	Tak
8.	Obsługa MIB	Tak
II. OCHRONA		
9.	Funkcje DHCP	DHCP relay, DHCP server, DHCPv6 client
10.	Lista kontrolna dostępu (ACL)	Tak
11.	Zasady Listy Kontroli Dostępu (ACL)	1024
12.	IGMP snooping	Tak
13.	Ochrona hasłem	Tak
14.	obsługuje SSH/SSL	Tak
15.	Filtrowanie adresów MAC	Tak
16.	Szyfrowanie / bezpieczeństwo	HTTPS, SSH, SSL/TLS
III. PORTY I INTERFEJSY		
17.	Podstawowe przełączanie RJ-45 Liczba portów Ethernet	48
18.	Podstawowe przełączania Ethernet RJ-45 porty typ	Gigabit Ethernet (10/100/1000)
19.	Ilość slotów Modułu SFP+	4

I-I.271.11.2024 Gorzyce, 15.07.2024 r.

20.	Liczba portów USB 2.0	1
IV. SIEĆ		
21.	Standardy komunikacyjne	IEEE 802.1D, IEEE 802.1w, IEEE 802.1s, IEEE 802.3, IEEE 802.3u, IEEE 802.3ab, IEEE 802.3z, IEEE 802.3ad
22.	Obsługa 10G	Tak
23.	Dublowanie portów	Tak
24.	Protokół drzewa rozpinającego	Tak
25.	Blokowanie head-of-line (HOL)	Tak
26.	Prędkość transferu danych przez Ethernet LAN	10,100,1000 Mbit/s
27.	Kontrola wzrostu natężenia ruchu	Tak
28.	Automatyczne MDI/MDI-X	Tak
29.	Podpora kontroli przepływu	Tak
30.	Agregator połączenia	Tak
31.	Obsługa sieci VLAN	Tak
32.	Liczba VLANs	4094
V. PRZESYŁANIE DANYCH		
33.	Wielkość tabeli adresów	16000 wejścia

34.	Zgodny z Jumbo Frames	Tak
35.	Rozszerzenie Jumbo Frames	9000
VI. FUNKCJE MULTICAST		
36.	Obsługa Multicast	Tak
VII. PROTOKOŁY		
37.	Protokoły zarządzające	SNMP
VIII. KONSTRUKCJA		
38.	Możliwości montowania w stelażu	Tak
39.	Przycisk reset	Tak
40.	Diody LED	Tak
IX. WYDAJNOŚĆ		
41.	Procesor wbudowany	Tak
42.	Taktowanie procesora	800 MHz
43.	Pojemność pamięci wewnętrznej	512 MB
44.	Wielkość pamięci flash	256 MB
45.	Aktualizacje oprogramowania urządzenia	Tak
X. MOC		

46.	Zasilacz dołączony	Tak
XI. WARUNKI PRACY		
47.	Zakres temperatur (eksploatacja)	-5 - 50 °C
48.	Zakres temperatur (przechowywanie)	-25 - 70 °C
49.	Zakres wilgotności względnej	10 - 90%
50.	Dopuszczalna wilgotność względna	10 - 90%

7. UTM - 2 sztuki.

Wymagania Ogólne

System bezpieczeństwa realizuje wszystkie wymienione poniżej funkcje sieciowe i bezpieczeństwa niezależnie od dostawcy łącza. Poszczególne elementy wchodzące w skład systemu bezpieczeństwa mogą być zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub komercyjnych aplikacji instalowanych na platformach ogólnego przeznaczenia. W przypadku implementacji programowej muszą być zapewnione niezbędne platformy sprzętowe wraz z odpowiednio zabezpieczonym systemem operacyjnym. Dla wszystkich funkcji systemu musi być dostarczony dokument potwierdzony przez producenta lub autoryzwanego dytrybutora o gotowości świadczenia usług wsparcia w języku polskim oraz bezpłatnej obsługi procesu wymiany uszkodzonego urządzenia.

System realizujący funkcję Firewall zapewnia pracę w jednym z trzech trybów: Routera z funkcją NAT, transparentnym oraz monitorowania na porcie SPAN.

System umożliwia budowę 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 wspiera protokoły 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 – istnieje możliwość łączenia w klaster Active-Active lub Active-Passive. W obu trybach system firewall zapewnia funkcję synchronizacji sesji.
2. Monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łączy sieciowych.
3. Monitoring stanu realizowanych połączeń VPN.
4. System umożliwia agregację linków statyczną oraz w oparciu o protokół LACP. Ponadto daje możliwość tworzenia interfejsów redundantnych.

Interfejsy, Dysk, Zasilanie:

1. System realizujący funkcję Firewall dysponuje co najmniej poniższą liczbą i rodzajem interfejsów:

- 10 portami Gigabit Ethernet RJ-45.

2. System Firewall posiada wbudowany port konsoli szeregowej oraz gniazdo USB umożliwiające podłączenie modemu 3G/4G oraz instalacji oprogramowania z klucza USB.
3. System Firewall pozwala skonfigurować co najmniej 200 interfejsów wirtualnych, definiowanych jako VLAN'y w oparciu o standard 802.1Q.
4. System jest wyposażony w zasilanie AC.

Parametry wydajnościowe:

1. W zakresie Firewall'a obsługa nie mniej niż 700 tys. jednoczesnych połączeń oraz 32 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 protokołem AES z kluczem 128 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 1.3 Gbps.
6. Wydajność skanowania ruchu typu Enterprise Mix z włączonymi funkcjami: IPS, Application Control, Antywirus - minimum 650 Mbps.
7. Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL dla ruchu http – minimum 600 Mbps.

Funkcje Systemu Bezpieczeństwa:

W ramach systemu ochrony są realizowane wszystkie poniższe funkcje. Mogą one być 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.
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. Konieczne są 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. Inspekcja (minimum: IPS) ruchu szyfrowanego protokołem SSL/TLS, minimum dla następujących typów ruchu: HTTP (w tym HTTP/2), SMTP, FTP, POP3.
12. Funkcja lokalnego serwera DNS z możliwością filtrowania zapytań DNS na lokalnym serwerze DNS jak i w ruchu przechodzącym przez system.
13. Rozwiązanie posiada wbudowane mechanizmy automatyzacji polegające na wykonaniu określonej sekwencji akcji (takich jak zmiana konfiguracji, wysłanie powiadomień do administratora) po wystąpieniu wybranego zdarzenia (np. naruszenie polityki bezpieczeństwa).

Polityki, Firewall

1. Polityka Firewall uwzględnia: adresy IP, użytkowników, protokoły, usługi sieciowe, aplikacje lub zbiory aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń.
2. System realizuje 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 istnieje możliwość tworzenia wydzielonych stref bezpieczeństwa np. DMZ, LAN, WAN.
4. Możliwość wykorzystania w polityce bezpieczeństwa zewnętrznych repozytoriów zawierających: kategorie URL, adresy IP.

5. Polityka firewall umożliwia filtrowanie ruchu w zależności od kraju, do którego przypisane są adresy IP źródłowe lub docelowe.
6. Możliwość ustawienia przedziału czasu, w którym dana reguła w politykach firewall jest aktywna.
7. Element systemu realizujący funkcję Firewall integruje 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.
   - Cisco ACI.
   - Google Cloud Platform (GCP).
   - OpenStack.
   - VMware NSX.
   - Kubernetes.

Połączenia VPN

1. System umożliwia konfigurację połączeń typu IPSec VPN. W zakresie tej funkcji zapewnia:
   - Wsparcie dla IKE v1 oraz v2.
   - Obsługę szyfrowania protokołem minimum AES z kluczem 128 oraz 256 bitów w trybie pracy Galois/Counter Mode(GCM).
   - Obsługa protokołu Diffie-Hellman grup 19, 20.
   - Wsparcie dla Pracy w topologii Hub and Spoke oraz Mesh.
   - 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.
   - Wsparcie dla następujących typów uwierzytelniania: pre-shared key, certyfikat.
   - Możliwość ustawienia maksymalnej liczby tuneli IPSec negocjowanych (nawiązywanych) jednocześnie w celu ochrony zasobów systemu.
   - Możliwość monitorowania wybranego tunelu IPSec site-to-site i w przypadku jego niedostępności automatycznego aktywowania zapasowego tunelu.
   - Obsługę mechanizmów: IPSec NAT Traversal, DPD, Xauth.
   - Mechanizm „Split tunneling" dla połączeń Client-to-Site.
2. System umożliwia konfigurację połączeń typu SSL VPN. W zakresie tej funkcji zapewnia:
   - Pracę w trybie Portal - gdzie dostęp do chronionych zasobów realizowany jest za pośrednictwem przeglądarki. W tym zakresie system zapewnia 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 posiada w ofercie oprogramowanie klienckie VPN, które umożliwia realizację połączeń IPSec VPN lub SSL VPN. Oprogramowanie klienckie vpn jest dostępne jako opcja i nie jest wymagane w implementacji.

Routing i obsługa łączy WAN

W zakresie routingu rozwiązanie zapewnia obsługę:

1. Routingu statycznego.
2. Policy Based Routingu (w tym: wybór trasy w zależności od adresu źródłowego, protokołu sieciowego, oznaczeń Type of Service w nagłówkach IP).
3. Protokołów dynamicznego routingu w oparciu o protokoły: RIPv2 (w tym RIPng), OSPF (w tym OSPFv3), BGP oraz PIM.
4. Możliwość filtrowania tras rozgłaszanych w protokołach dynamicznego routingu.
5. ECMP (Equal cost multi-path) – wybór wielu równoważnych tras w tablicy routingu.

6. BFD (Bidirectional Forwarding Detection).
7. Monitoringu dostępności wybranego adresu IP z danego interfejsu urządzenia i w przypadku jego niedostępności automatyczne usunięcie wybranych tras z tablicy routingu.

Funkcje SD-WAN

1. System umożliwia wykorzystanie protokołów dynamicznego routingu przy konfiguracji równoważenia obciążenia do łączy WAN.
2. SD-WAN wspiera zarówno interfejsy fizyczne jak i wirtualne (w tym VLAN, IPSec).

Zarządzanie pasmem

1. System Firewall umożliwia zarządzanie pasmem poprzez określenie: maksymalnej i gwarantowanej ilości pasma, oznaczanie DSCP oraz wskazanie priorytetu ruchu.
2. System daje możliwość określania pasma dla poszczególnych aplikacji.
3. System pozwala zdefiniować pasmo dla wybranych użytkowników niezależnie od ich adresu IP.
4. System zapewnia możliwość zarządzania pasmem dla wybranych kategorii URL.

Ochrona przed malware

1. Silnik antywirusowy umożliwia skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021).
2. Silnik antywirusowy zapewnia skanowanie następujących protokołów: HTTP, HTTPS, FTP, POP3, IMAP, SMTP, CIFS.
3. System umożliwia skanowanie archiwów, w tym co najmniej: Zip, RAR. W przypadku archiwów zagnieżdżonych istnieje możliwość określenia, ile zagnieżdżeń kompresji system będzie próbował zdekompresować w celu przeskanowania zawartości.
4. System umożliwia blokowanie i logowanie archiwów, które nie mogą zostać przeskanowane, ponieważ są zaszyfrowane, uszkodzone lub system nie wspiera inspekcji tego typu archiwów.
5. System dysponuje sygnaturami do ochrony urządzeń mobilnych (co najmniej dla systemu operacyjnego Android).
6. Baza sygnatur musi być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.
7. System współpracuje z dedykowaną platformą typu Sandbox lub usługą typu Sandbox realizowaną
w chmurze. Konieczne jest zastosowanie platformy typu Sandbox wraz z niezbędnymi serwisami lub licencjami upoważniającymi do korzystania z usługi typu Sandbox w chmurze.
8. System zapewnia usuwanie aktywnej zawartości plików PDF oraz Microsoft Office bez konieczności blokowania transferu całych plików.
9. Możliwość wykorzystania silnika sztucznej inteligencji AI wytrenowanego przez laboratoria producenta.
10. Możliwość uruchomienia ochrony przed malware dla wybranego zakresu ruchu.

Ochrona przed atakami

1. Ochrona IPS opiera się co najmniej na analizie sygnaturowej oraz na analizie anomalii w protokołach sieciowych.
2. System chroni przed atakami na aplikacje pracujące na niestandardowych portach.
3. Baza sygnatur ataków zawiera minimum 5000 wpisów i jest aktualizowana automatycznie, zgodnie
z harmonogramem definiowanym przez administratora.
4. Administrator systemu ma możliwość definiowania własnych wyjątków oraz własnych sygnatur.
5. System zapewnia 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).
7. Możliwość kontrolowania długości nagłówka, ilości parametrów URL oraz Cookies dla protokołu http.

8. Wykrywanie i blokowanie komunikacji C&C do sieci botnet.
9. Możliwość uruchomienia ochrony przed atakami dla wybranych zakresów komunikacji sieciowej. Mechanizmy ochrony IPS nie mogą działać globalnie.

Kontrola aplikacji

1. Funkcja Kontroli Aplikacji umożliwia kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP.
2. Baza Kontroli Aplikacji zawiera minimum 2000 sygnatur i jest aktualizowana automatycznie, zgodnie
z harmonogramem definiowanym przez administratora.
3. Aplikacje chmurowe (co najmniej: Facebook, Google Docs, Dropbox) są kontrolowane pod względem wykonywanych czynności, np.: pobieranie, wysyłanie plików.
4. Baza sygnatur zawiera kategorie aplikacji szczególnie istotne z punktu widzenia bezpieczeństwa: proxy, P2P.
5. Administrator systemu ma możliwość definiowania wyjątków oraz własnych sygnatur.
6. Istnieje możliwość blokowania aplikacji działających na niestandardowych portach (np. FTP na porcie 2021).
7. System daje możliwość określenia dopuszczalnych protokołów na danym porcie TCP/UDP i blokowania pozostałych protokołów korzystających z tego portu (np. dopuszczenie tylko HTTP na porcie 80).

Kontrola WWW

1. Moduł kontroli WWW korzysta z bazy zawierającej co najmniej 40 milionów adresów URL pogrupowanych w kategorie tematyczne.
2. W ramach filtra WWW są dostępne kategorie istotne z punktu widzenia bezpieczeństwa, jak: malware (lub inne będące źródłem złośliwego oprogramowania), phishing, spam, Dynamic DNS, proxy.
3. Filtr WWW dostarcza kategorii stron zabronionych prawem np.: Hazard.
4. Administrator ma możliwość nadpisywania kategorii oraz tworzenia wyjątków – białe/czarne listy dla adresów URL.
5. Filtr WWW umożliwia statyczne dopuszczanie lub blokowanie ruchu do wybranych stron WWW,
w tym pozwala definiować strony z zastosowaniem wyrażeń regularnych (Regex).
6. Filtr WWW daje możliwość wykonania akcji typu „Warning” – ostrzeżenie użytkownika wymagające od niego potwierdzenia przed otwarciem żądanej strony.

a) Funkcja Safe Search – przeciwdziałająca pojawieniu się niechcianych treści w wynikach wyszukiwarek takich jak: Google oraz Yahoo.
b) Administrator ma możliwość definiowania komunikatów zwracanych użytkownikowi dla różnych akcji podejmowanych przez moduł filtrowania WWW.
c) System pozwala określić, dla których kategorii URL lub wskazanych URL nie będzie realizowana inspekcja szyfrowanej komunikacji.

Uwierzytelnianie użytkowników w ramach sesji

1. System Firewall umożliwia 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. System daje możliwość zastosowania w tym procesie uwierzytelniania dwuskładnikowego.
3. System umożliwia budowę architektury uwierzytelniania typu Single Sign On przy integracji ze środowiskiem Active Directory oraz zastosowanie innych mechanizmów: RADIUS, API lub SYSLOG w tym procesie.

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 mogą współpracować z dedykowanymi platformami centralnego zarządzania i monitorowania.
2. Komunikacja elementów systemu zabezpieczeń z platformami centralnego zarządzania jest realizowana z wykorzystaniem szyfrowanych protokołów.
3. Istnieje możliwość włączenia mechanizmów uwierzytelniania dwu-składnikowego dla dostępu administracyjnego.
4. System współpracuje z rozwiązaniami monitorowania poprzez protokoły SNMP w wersjach 2c, 3 oraz umożliwia przekazywanie statystyk ruchu za pomocą protokołów Netflow lub sFlow.
5. System daje możliwość zarządzania przez systemy firm trzecich poprzez API, do którego producent udostępnia dokumentację.
6. Element systemu pełniący funkcję Firewall posiada wbudowane narzędzia diagnostyczne, przynajmniej: ping, traceroute, podglądu pakietów, monitorowanie procesowania sesji oraz stanu sesji firewall.
7. Element systemu realizujący funkcję Firewall umożliwia wykonanie szeregu zmian przez administratora w CLI lub GUI, które nie zostaną zaimplementowane zanim nie zostaną zatwierdzone.
8. Możliwość przypisywania administratorom praw do zarządzania określonymi częściami systemu (RBM).
9. Możliwość zarządzania systemem tylko z określonych adresów źródłowych IP.

Logowanie

Elementy systemu bezpieczeństwa realizują logowanie do aplikacji (logowania i raportowania) udostępnianej w chmurze, lub konieczne jest zastosowanie komercyjnego systemu logowania i raportowania w postaci odpowiednio zabezpieczonej, komercyjnej platformy sprzętowej lub programowej.

1. W ramach logowania element systemu pełniący funkcję Firewall zapewnia przekazywanie danych
o: zaakceptowanym ruchu, blokowanym ruchu, aktywności administratorów, zużyciu zasobów oraz stanie pracy systemu. Ponadto zapewnia możliwość jednoczesnego wysyłania logów do wielu serwerów logowania.
2. Logowanie obejmuje zdarzenia dotyczące wszystkich modułów sieciowych i bezpieczeństwa.
3. Możliwość włączenia logowania per reguła w polityce firewall.
4. System zapewnia możliwość logowania do serwera SYSLOG.
5. Przesyłanie SYSLOG do zewnętrznych systemów jest możliwe z wykorzystaniem protokołu TCP oraz szyfrowania SSL/TLS.

Testy wydajnościowe oraz funkcjonalne

Wszystkie funkcje i parametry wydajnościowe systemu mogą być zweryfikowane w oparciu o oficjalną (publicznie dostępną) dokumentację producenta oraz wykonane testy.

Serwisy i licencje

Do korzystania z aktualnych baz funkcji ochronnych producenta i serwisów wymagane są licencje:

Kontrola Aplikacji, IPS, Antywirus (z uwzględnieniem sygnatur do ochrony urządzeń mobilnych - co najmniej dla systemu operacyjnego Android), Analiza typu Sandbox cloud, Antyspam, Web Filtering, bazy reputacyjne adresów IP/domen na okres 24 miesięcy.

Gwarancja oraz wsparcie

System jest objęty serwisem gwarancyjnym producenta przez okres 24 miesięcy, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości w trybie AHR (advanced hardware replacement). W ramach tego serwisu producent zapewnia dostęp do aktualizacji oprogramowania oraz wsparcie techniczne w trybie 24x7.

I-I.271.11.2024 Gorzyce, 15.07.2024 r.

Opisy do wymagań ogólnych

1. Zaleca się, aby w przypadku istnienia takiego wymogu w stosunku do technologii objętej przedmiotem niniejszego postępowania (tzw. produkty podwójnego zastosowania), został uzyskany 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. Zaleca się, aby został uzyskany dokument - oświadczenie producenta lub autoryzowanego dystrybutora producenta na terenie Polski, iż produkt pochodzi z autoryzowanego kanału sprzedaży, np. poprzez oświadczenie o posiadanym statusie autoryzacyjnym.

8. Macierz dyskowa - 1 sztuka.

Element konfiguracji/cecha/funkcjonalność	**Wymagania minimalne**
Typ obudowy	Macierz musi być przystosowana do montażu w szafie rack 19”, o wysokość maksymalnie 2U oraz umożliwiać montaż min. 12 dysków 3.5”
Przestrzeń dyskowa	Zainstalowane: 6x dysk SAS o pojemności min. 2.4TB, Hot-Plug 6x dysk SAS o pojemności min. 16TB, Hot-Plug
Możliwość rozbudowy	Macierz musi umożliwiać rozbudowę (bez wymiany kontrolerów macierzy), do co najmniej 264 dysków twardych.
Obsługa dysków	Macierz musi mieć możliwość obsługiwania dysków SSD, SAS i Nearline SAS. Macierz musi umożliwiać mieszanie napędów dyskowych SSD, SAS i NL SAS w obrębie pojedynczej półki dyskowej. Macierz musi obsługiwać dyski 2,5” jak również 3,5”.
Sposób zabezpieczenia danych	Macierz musi obsługiwać mechanizmy RAID zgodne z RAID0, RAID1, RAID10, RAID5, RAID6 oraz RAID z tzw. rozproszoną wolną pojemnością, realizowane sprzętowo za pomocą dedykowanego układu, z możliwością dowolnej ich kombinacji w obrębie oferowanej macierzy i z wykorzystaniem wszystkich dysków (tzw. wide-striping). Macierz musi umożliwiać definiowanie globalnych dysków spare oraz dedykowanie dysków spare do konkretnych grup RAID.

I-I.271.11.2024 Gorzyce, 15.07.2024 r.

	Macierz musi również oferować możliwość zdefiniowania grup dyskowych z tzw. rozproszoną wolną pojemnością, która nie wykorzystuje tradycyjnych dysków zapasowych (integracja dysków zapasowych i nieaktywnych do zwiększenia dostępności i wydajności macierzy, zwiększenie szybkości odbudowy macierzy na wypadek awarii dysku). Macierz musi umożliwiać obsługę dysków różnej pojemności w ramach grupy dysków.
Tryb pracy kontrolerów macierzowych	Macierz musi posiadać minimum 2 kontrolery macierzowe pracujące w trybie active-active i udostępniające jednocześnie dane blokowe. Wszystkie kontrolery muszą komunikować się między sobą bez stosowania dodatkowych przełączników lub koncentratorów.
Pamięć cache	Macierz musi posiadać minimum sumarycznie 32 GB pamięci cache. Pamięć cache musi być zbudowana w oparciu o wydajną pamięć typu RAM. Pamięć zapisu musi być mirrorowana (kopie lustrzane) pomiędzy kontrolerami dyskowymi. Dane niezapisane na dyskach (np. zawartość pamięci kontrolera) muszą zostać zabezpieczone w przypadku awarii zasilania za pomocą podtrzymania bateryjnego lub z zastosowaniem innej technologii przez okres minimum 5 lat.
Rozbudowa pamięci cache	Macierz musi umożliwiać zwiększenie pojemności pamięci cache dla odczytów do minimum 8 TB z wykorzystaniem dysków SSD lub kart pamięci flash. Jeżeli do obsługi powyższej funkcjonalności wymagane są dodatkowe licencje, należy je dostarczyć wraz z rozwiązaniem.
Interfejsy	Macierz musi posiadać, co najmniej 8 portów iSCSI 25Gb (4 porty na kontroler),
Kable/wkładki	4x kabel DAC 25GbE SFP28-SFP28 min. 5m
Zarządzanie	Zarządzanie macierzą musi być możliwe z poziomu interfejsu graficznego i interfejsu znakowego. Zarządzanie macierzą musi odbywać się bezpośrednio na kontrolerach macierzy z poziomu przeglądarki internetowej.

I-I.271.11.2024 Gorzyce, 15.07.2024 r.

Zarządzanie grupami dyskowymi oraz dyskami logicznymi	Macierz musi umożliwiać zdefiniowanie, co najmniej 500 wolumenów logicznych w ramach oferowanej macierzy dyskowej. Musi istnieć możliwość rozłożenia pojedynczego wolumenu logicznego na wszystkie dyski fizyczne macierzy (tzw. wide-striping), bez konieczności łączenia wielu różnych dysków logicznych w jeden większy. Jeżeli do obsługi powyższych funkcjonalności wymagane są dodatkowe licencje, należy je dostarczyć dla całej pojemności urządzenia.
Thin Provisioning	Macierz musi umożliwiać udostępnianie zasobów dyskowych do serwerów w trybie tradycyjnym, jak i w trybie typu Thin Provisioning. Macierz musi umożliwiać odzyskiwanie przestrzeni dyskowych po usuniętych danych w ramach wolumenów typu Thin. Proces odzyskiwania danych musi być automatyczny bez konieczności uruchamiania dodatkowych procesów na kontrolerach macierzowych (wymagana obsługa standardu T10 SCSI UNMAP). Jeżeli do obsługi powyższych funkcjonalności wymagane są dodatkowe licencje, należy je dostarczyć dla całej pojemności urządzenia.
Tiering	Macierz musi posiadać funkcjonalność Tiering między dyskami SSD i SAS i między dyskami SAS i NL SAS. Tiering musi obejmować wszystkie woluminy w danej puli dyskowej. Dyski SSD mogą być wykorzystane zarówno do uzyskania pojemności w warstwie wydajności lub na potrzeby zwiększenia pamięci podręcznej odczytu w celu przyspieszenia operacji losowego odczytu z jednej lub wielu warstw napędów mechanicznych.
Wewnętrzne kopie migawkowe	Macierz musi umożliwiać dokonywania na żądanie tzw. migawkowej kopii danych (snapshot, point-in-time) w ramach macierzy za pomocą wewnętrznych kontrolerów macierzowych. Kopia migawkowa wykonuje się bez alokowania dodatkowej przestrzeni dyskowej na potrzeby kopii. Zajmowanie dodatkowej przestrzeni dyskowej następuje w momencie zmiany danych na dysku źródłowym lub na jego kopii. Macierz musi wspierać minimum 512 kopii migawkowych. Jeżeli do obsługi powyższych funkcjonalności wymagane są dodatkowe licencje, należy je dostarczyć dla całej pojemności urządzenia.
Wewnętrzne kopie pełne	Macierz musi umożliwiać dokonywanie na żądanie pełnej fizycznej kopii danych (clone) w ramach macierzy za pomocą wewnętrznych kontrolerów macierzowych.

I-I.271.11.2024 Gorzyce, 15.07.2024 r.

	Jeżeli do obsługi powyższych funkcjonalności wymagane są dodatkowe licencje, należy je dostarczyć dla całej pojemności urządzenia.
Migracja danych w obrębie macierzy	Macierz dyskowa musi umożliwiać migrację danych bez przerywania do nich dostępu pomiędzy różnymi warstwami technologii dyskowych na poziomie części wolumenów logicznych (ang. Sub-LUN). Zmiany te muszą się odbywać wewnętrznymi mechanizmami macierzy. Funkcjonalność musi umożliwiać zdefiniowanie zasobu LUN, który fizycznie będzie znajdował się na min. 3 typach dysków obsługiwanych przez macierz, a jego części będą realokowane na podstawie analizy ruchu w sposób automatyczny i transparentny (bez przerywania dostępu do danych) dla korzystających z tego wolumenu hostów. Zmiany te muszą się odbywać wewnętrznymi mechanizmami macierzy. Jeżeli do obsługi powyższych funkcjonalności wymagane są dodatkowe licencje, należy je dostarczyć dla całej pojemności dostarczanego urządzenia.
Zdalna replikacja danych	Macierz musi umożliwiać asynchroniczną replikację danych do innej macierzy z tej samej rodziny. Replikacja musi być wykonywana na poziomie kontrolerów, bez użycia dodatkowych serwerów lub innych urządzeń i bez obciążania serwerów podłączonych do macierzy. Jeżeli do obsługi powyższej funkcjonalności wymagane są dodatkowe licencje, należy je dostarczyć wraz z urządzeniem.
Podłączanie zewnętrznych systemów operacyjnych	Macierz musi umożliwiać jednoczesne podłączenie wielu serwerów w trybie wysokiej dostępności (co najmniej dwoma ścieżkami). Macierz musi wspierać podłączenie następujących systemów operacyjnych: Windows, RHEL, SLES, Vmware, Citrix. Dla wymienionych systemów operacyjnych należy dostarczyć oprogramowanie do przełączania ścieżek i równoważenia obciążenia poszczególnych ścieżek. Wymagane jest oprogramowanie dla nielimitowanej liczby serwerów. Dopuszcza się rozwiązania bazujące na natywnych możliwościach systemów operacyjnych. Jeżeli do obsługi powyższych funkcjonalności wymagane są dodatkowe licencje, należy je dostarczyć dla maksymalnej liczby serwerów obsługiwanych przez oferowane urządzenie.
Redundancja	Macierz nie może posiadać pojedynczego punktu awarii, który powodowałby brak dostępu do danych. Musi być zapewniona pełna redundancja komponentów, w szczególności zdublowanie kontrolerów, zasilaczy i wentylatorów.

I-I.271.11.2024 Gorzyce, 15.07.2024 r.

	Macierz musi umożliwiać wymianę elementów systemu w trybie „hot-swap", a w szczególności takich, jak: dyski, kontrolery, zasilacze, wentylatory. Macierz musi mieć możliwość zasilania z dwu niezależnych źródeł zasilania – odporność na zanik zasilania jednej fazy lub awarię jednego z zasilaczy macierzy. Zasilacze użyte w macierzy powinny posiadać certyfikat sprawności zasilacza minimum 80+ Gold.
Dodatkowe wymagania	Oferowany system dyskowy musi się składać z pojedynczej macierzy dyskowej. Niedopuszczalna jest realizacja zamówienia poprzez dostarczenie wielu macierzy dyskowych. Za pojedynczą macierz nie uznaje się rozwiązania opartego o wiele macierzy dyskowych (par kontrolerów macierzowych) połączonych przełącznikami SAN lub tzw. wirtualizatorem sieci SAN czy wirtualizatorem macierzy dyskowych. Możliwość ograniczania poboru zasilania przez dyski, które nie obsługują operacji we/wy, poprzez ich zatrzymanie.
Standardy bezpieczeństwa	Urządzenie musi spełniać następujące standardy bezpieczeństwa: EN 62368-1 (European Union), IEC 60950-1 (International)
Inne	Urządzenia muszą być zakupione w oficjalnym kanale dystrybucyjnym producenta. Na żądanie Zamawiającego, Wykonawca musi przedstawić oświadczenie producenta oferowanego serwera, potwierdzające pochodzenie urządzenia z oficjalnego kanału dystrybucyjnego producenta. Wymagane są dokumenty poświadczające, że sprzęt jest produkowany zgodnie z normami ISO 9001 oraz ISO 14001. Deklaracja zgodności CE.
Warunki gwarancji	5 lat gwarancji producenta Zamawiający oczekuje możliwości zgłaszania zdarzeń serwisowych w trybie 24/7/365 następującymi kanałami: telefonicznie, przez Internet oraz z wykorzystaniem aplikacji. Zamawiający oczekuje rozpoczęcia diagnostyki telefonicznej / internetowej już w momencie dokonania zgłoszenia. Certyfikowany Technik wykonawcy / producenta z właściwym zestawem części do naprawy (potwierdzonym na etapie diagnostyki) ma rozpocząć naprawę w siedzibie zamawiającego najpóźniej w następnym dniu roboczym (NBD) od otrzymania zgłoszenia / zakończenia diagnostyki.

	Naprawa ma się odbywać w siedzibie zamawiającego, chyba, że zamawiający dla danej naprawy zgodzi się na inną formę. Zamawiający oczekuje bezpośredniego dostępu do wykwalifikowanej kadry inżynierów technicznych. Zamawiający wymaga pojedynczego punktu kontaktu dla całego rozwiązania producenta, w tym także sprzedanego oprogramowania. Zgłoszenie przyjęte jest potwierdzane przez zespół pomocy technicznej (mail/telefon / aplikacja / portal) przez nadanie unikalnego numeru zgłoszenia pozwalającego na identyfikację zgłoszenia w trakcie realizacji naprawy i po jej zakończeniu. Możliwość sprawdzenia statusu gwarancji poprzez stronę producenta podając unikatowy numer urządzenia oraz pobieranie uaktualnień mikrokodu oraz sterowników nawet w przypadku wygaśnięcia gwarancji urządzenia. Zamawiający oczekuje nieodpłatnego udostępnienia narzędzi serwisowych i procesów wsparcia umożliwiających: Wykrywanie usterek sprzętowych z predykcją awarii. Automatyczną diagnostykę i zdalne otwieranie zgłoszeń serwisowych. Zamawiający wymaga od podmiotu realizującego serwis lub producenta sprzętu dołączenia do oferty oświadczenia, że w przypadku wystąpienia awarii dysku twardego w urządzeniu objętym aktywnym wparciem technicznym, uszkodzony dysk twardy pozostaje u Zamawiającego. Możliwość rozszerzenia gwarancji przez producenta do 7 lat. Firma serwisująca musi posiadać ISO 9001:2015 oraz ISO-27001 na świadczenie usług serwisowych oraz posiadać autoryzacje producenta urządzeń – dokumenty potwierdzające należy załączyć do oferty. Wymagane dołączenie do oferty oświadczenia Producenta potwierdzając, że Serwis urządzeń będzie realizowany bezpośrednio przez Producenta i/lub we współpracy z Autoryzowanym Partnerem Serwisowym Producenta.

9. UPS - 1 sztuka.

Lp.	Nazwa elementu, parametru lub cechy	Opis wymagań
1 .	Moc pozorna	3000VA
2 .	Moc rzeczywista	3000W

I-I.271.11.2024 Gorzyce, 15.07.2024 r.

3 .	Topologia (klasyfikacja IEC 62040-3)	Podwójna konwersja on-line z korekcją wejściowego współczynnika mocy systemu (PFC)
4 .	Sprawność przy pracy normalnej (100% obc.)	<94%
5 .	Sprawność w trybie podwyższonej sprawności (100% obc.)	>98%
6 .	Współczynnik mocy	1
7 .	Czas przełączenia na baterię	0 ms
8.	Możliwość pracy równoległej	tak
9.	Liczba, typ gniazd wyjściowych	8 gniazd IEC C13 (10A) + 2 gniazda IEC C19 (16A), w tym 2 zarządzalne grupy wraz z pomiarem zużytej energi
10.	Typ gniazda wejściowego	1 IEC C20 (16A) lub blok zacisków w wersji HotSwap MBP HW
11.	Czas podtrzymania dla 100% obciążenia dla pf=1	3 min
12.	Czas podtrzymania przy 50% obciążenia dla pf=1	10 min
13.	Dodatkowe baterie	Możliwość dołożenia maksymalnie 4 zewnętrznych modułów bateryjnych
14.	Napięcie znamionowe	200/208/220/230/240 V
15.	Tolerancja napięci prostownika	176V – 276 V (100-276V przy <33% obciążeniu)
16.	Częstotliwość znamionowa	50/60 Hz autodetekcja

I-I.271.11.2024 Gorzyce, 15.07.2024 r.

17.	Tolerancja częstotliwości	40– 70 Hz
18.	Kształt napięcia	Sinusoidalny
19.	Napięcie znamionowe wyjściowe	230 V (domyślnie) / możliwość wyboru 200/208/220/240 V
20.	Zakres zmian napięcia	+/-1% napięcia nominalnego
21.	Częstotliwość wyjściowa	50/60 Hz +/-0,5%
22.	Współczynnik szczytu	3:1
23.	Dopuszczalny zakres współczynnika mocy obc. Liniowego	0,5 indukcyjny - 0,5 pojemnościowy
24.	Baterie wymieniane przez użytkownika "na gorąco"	Tak
25.	Ochrona przed przeładowaniem	Tak (ograniczenie prądu ładowarki, wyłączenie ładowarki / alarm)
26.	Ochrona przed głębokim rozładowaniem	Tak
27.	Okresowy automatyczny test baterii	Tak
28.	System zarządzania pracą baterii	System nieciągłego ładowania baterii. Do oferty dołączyć należy opis algorytmu ładowania nieciągłego baterii. W opisie znaleźć się muszą informacje nt. trwania okresów ładowania forsującego, konserwującego i okresu spoczynkowego (tzw. restingu). Okres spoczynkowy w jednym cyklu nie może być krótszy niż 14 dni. Opis powinien być materiałem firmowym producenta lub musi być przez niego potwierdzony.
29.	Zdolność zwarciowa	90A

I-I.271.11.2024 Gorzyce, 15.07.2024 r.

30.	Możliwość uruchomienia bez napięcia w sieci	Tak
31.	Baterie wewnętrzne o pojemności nie mniejszej niż	9Ah 12V, minimum 6 szt.
32.	Czas ładowania baterii do poziomu 90%	< 1,5 godz. do 90% pojemności użytkowej
33.	Interfejs komunikacyjny	• USB
		• RS232 DB-9 żeński (HID)
		• 1 blok mini-zacisków dla zdalnego załączania/wyłączania
		• 1 blok mini-zacisków do zdalnego wyłączania
		• 1 blok mini-zacisków przekaźnika wyjściowego
34.	Panel sterowania z wyświetlaczem LCD	• Panel LCD obrotowy (do ułatwienia odczytów przy obu wariantach montażu UPSa). Dostarcza informacji o : stanie pracy urządzenia, stanie obciążenia, pomiarach i ustawieniach. Funkcje ustawień i odczytów: lokalne, wyjścia (napięcie wyjściowe , częstotliwość wyjściowa), baterii (test baterii), pomiary i dane (numer seryjny, napięcie i częstotliwość wejściowa i wyjściowa, poziom obciążenia, pozostały czas podtrzymania, wydajność, zużycie energii).
		• Poziomy rząd przycisków sterowania
		• Poziomy rząd wskaźników stanu : 4 LED
		• Sygnalizator akustyczny
35.	Sygnały akustyczne	• Awaria

I-I.271.11.2024 Gorzyce, 15.07.2024 r.

		• Niski stan naładowania baterii
		• Przeciążenie
		• Serwis
36.	Przyciski sterujące i wskaźniki diodowe LED	• Przycisk Escape (anulowanie)
		• Przyciski funkcyjne (przewijanie w górę i w dół)
		• Przycisk Enter (potwierdzający)
		• Przycisk ON/OFF załączenia i wyłączenia
		• LED trybu zasilania z siec i(kolor zielony)
		• LED trybu baterii (kolor żółty)
		• LED usterki (kolor czerwony)
		• LED w trybie obejścia (kolor pomarańczowy)
37.	Kolor	Czarny RAL 9005
38.	Typ obudowy	Uniwersalna Tower/Rack 2U
39.	Wyposażenie standardowe	UPS, instrukcja obsługi(CD), instrukcja bezpieczeństwa, instrukcja szybkiego montażu
		1 x kabel szeregowy RS-232,
		1 x kabel komunikacyjny USB

		1 x kable wyjściowe IEC 16A
		2 x kable wyjściowe IEC 10A
		uchwyty kablowe
		1 x zestaw szyn montażowych 19’
		podstawki do montażu wieżowego
40.	Dołączone oprogramowanie	Tak, monitorujące i zarządzające UPS, umożliwiające automatyczne zamykanie serwerów zasilanych z systemu i pracujących pod kontrolą systemów operacyjnych: - Windows: 7 / 8 / 2008 / Vista / 2003 / XP - Microsoft SCVMM 2012 - Linux: Debian GNU Linux: Lenny, SUSE/Novell: SLES 11, OpenSUSE 11.2, Redhat Enterprise Linux: RHEL 5.3, 5.4, 5.5, Fedora core 12, Ubuntu: 10.04 - VMWare: vCenter / ESXi 5.1 - Citrix XEN 6.0
41.	Zgodność ze standardem Energy Star	Tak
42.	Maksymalna szerokość	440 mm
43.	Maksymalna wysokość	86,5 mm
44.	Maksymalna głębokość	605 mm
45.	Maksymalny ciężar	27,4 kg
46.	Poziom hałasu w odl. 1m	<47 dBA dla pracy normalnej
47.	Znaki bezpieczeństwa	CE, C-Tick, IEC/EN 62040-1, IEC/EN 62040-2: Kat. C1, IEC/EN 62040-3

48.	Gwarancja producenta	3 lata na elektronikę, 2 lata na baterie akumulatorów

10. Oprogramowanie serwera - 4 sztuki.

Wymagane minimalne parametry

Oprogramowanie Windows Server 2022 Standard (licencja na 16 rdzeni procesora, wersja OEM) lub równoważne.

Opis równoważności dla systemu Windows Server 2022 Standard:

System operacyjny musi być przeznaczony do zastosowań serwerowych w Środowiskach fizycznych lub o minimalnej wirtualizacji.

System operacyjny musi być najnowszą wersją rodziny systemów operacyjnych danego producenta.

Licencja na system operacyjny musi uwzględniać prawo do bezpłatnej instalacji udostępnianych przez producenta poprawek krytycznych i opcjonalnych do zakupionej wersji oprogramowania co najmniej przez 5 lat.

Licencja na system operacyjny musi umożliwiać uruchomienie kontrolera domeny będącego w pełni zgodnym z domeną wdrożoną u Zamawiającego domeną Active Directory pracującą w oparciu o system Windows Server 2016 musi także być dostarczona możliwość uruchomienia roli kontrolera domeny Microsoft Active Directory na poziomie Microsoft Windows Server

Licencja na system operacyjny musi być bez ograniczeń czasowych.

Licencja na system operacyjny musi uprawniać do uruchamiania systemu operacyjnego w środowisku fizycznym i min. 2 środowiskach wirtualnych za pomocą wbudowanych mechanizmów wirtualizacji, bez konieczności zakupu dodatkowych licencji.

Zaimplementowanie w systemie operacyjnym środowiska wirtualizacyjnego musi umożliwiać dodawanie i usuwanie pamięci wirtualnej oraz wirtualnych kart sieciowych podczas pracy maszyny wirtualnej.

System operacyjny musi posiadać graficzny interfejs użytkownika.

System operacyjny musi być w pełni kompatybilny z usługą Active Directory w zakresie:

- zarządzania użytkownikami,
- zarządzania certyfikatami dla użytkowników wraz ze wsparciem możliwości logowania do domeny kartą mikroprocesorową,
- możliwości przydzielania praw dostępu do zasobów sieciowych,
- instalacji zdalnej oprogramowania z pakietów msi,
- definiowanie polityk bezpieczeństwa dla użytkowników, grup oraz stacji roboczych z systemami MS Windows: 7,8,8.1, 10,11.

System operacyjny musi wspierać pracę domenową wraz z automatyczną synchronizacją dla dodatkowych serwerów.

System operacyjny musi wspierać zarządzanie przez dostępne narzędzia administracji serwera dla systemu Windows 10 (RSAT) oraz Windows Admin Center.

System operacyjny musi posiadać obsługę zdalnego pulpitu poprzez protokół RDP.

System operacyjny musi umożliwiać ustawianie relacji zaufania pomiędzy domenami.

Wszystkie narzędzia i usługi systemu operacyjnego powinny być rozwiązaniem jednego producenta.

System operacyjny musi posiadać obsługę pamięci USB jako monitora klastra

System operacyjny musi pozwalać na stopniowe uaktualnienia systemu operacyjnego klastra

System operacyjny musi posiadać obsługę deduplikacji na potrzeby systemu plików ReFS.

System operacyjny musi posiadać obsługę optymalizacji transportu w tle pod kątem opóźnień.

System operacyjny musi posiadać wbudowaną zaporę internetową (firewall) dla ochrony połączeń internetowych; zapora musi być zintegrowana z systemem konsoli do zarządzania ustawieniami zapory i regułami ip v4 i v6;

System operacyjny musi posiadać możliwość uruchomienia serwera DNS z możliwością integracji z kontrolerem domeny;

I-I.271.11.2024 Gorzyce, 15.07.2024 r.

System operacyjny musi posiadać możliwość zdalnej automatycznej instalacji, konfiguracji, administrowania oraz aktualizowania systemu;
System operacyjny musi posiadać obsługa PowerShell 5.1,
System operacyjny musi posiadać obsługa certyfikatów w Active Directory
Wszystkie wymienione powyżej parametry, role, funkcje, itp. systemu operacyjnego objęte muszą być dostarczoną licencją (licencjami) i zawarte w dostarczonej wersji oprogramowania (nie wymagają ponoszenia przez Zamawiającego dodatkowych kosztów).

11. Licencje dostępowe - 40 sztuk.

1. Licencje dostępowe na użytkownika
   - Wymagana licencja typu Cal User OEM do systemu Windows Server 2022 (z niniejszego zamówienia) lub równoważne, jeśli oprogramowanie równoważne takich licencji wymaga.
2. Opis równoważności dla funkcjonalności dotyczące wymaganego przez Zamawiającego oprogramowania równoważnego do Windows Server 2022 na użytkownika:
   - Licencja dostępowa dla użytkownika umożliwiająca podłączenie i wykorzystywanie wszystkich dostępnych funkcjonalności serwera Microsoft Windows Server 2022 typu User Cal z wdrożoną rolą Active Directory

12. Oprogramowanie do wykonywania kopii zapasowych - 5 licencji uniwersalnych.

Licencja musi być na bezterminowa, bez żadnych dodatkowych opłat a wsparcie na minimum 12 miesięcy.

Lp.	Minimalne wymagania Zamawiającego
I. Wymagania ogólne	
1.	Oprogramowanie musi być produktem przeznaczonym do obsługi środowisk DataCenter. Oferowany produkt musi znajdować się w kwadracie liderów Gartner Magic Quadrant for Data Center Backup and Recovery Solutions oraz na ogólnie dostępnej liście referencyjnej Gartner: https://www.gartner.com/reviews/market/data-center-backup-and-recovery-solutions i spełniać minimalne wymaganie : - minimalna liczba referencji 150, - minimalna ocena z referencji 4,5
2.	Oprogramowanie musi współpracować z infrastrukturą VMware w wersji 6.x, 7.x i 8.0 oraz Microsoft Hyper-V 2012, 2012R2, 2016, 2019 i 2022. Wszystkie funkcjonalności w specyfikacji muszą być dostępne na wszystkich wspieranych platformach wirtualizacyjnych, chyba, że wyszczególniono inaczej
3.	Oprogramowanie musi zapewniać tworzenie kopii zapasowych z sieciowych urządzeń plikowych NAS opartych o SMB, CIFS i/lub NFS oraz bezpośrednio z serwerów plikowych opartych o Windows i Linux.
II. Całkowite koszty posiadania	
1.	Oprogramowanie musi być niezależne sprzętowo i umożliwiać wykorzystanie dowolnej platformy serwerowej i dyskowej

I-I.271.11.2024 Gorzyce, 15.07.2024 r.

2.	Oprogramowanie musi tworzyć “samowystarczalne” archiwa do odzyskania których nie wymagana jest osobna baza danych z metadanymi deduplikowanych bloków
3.	Oprogramowanie musi mieć mechanizmy deduplikacji i kompresji w celu zmniejszenia wielkości archiwów. Włączenie tych mechanizmów nie może skutkować utratą jakichkolwiek funkcjonalności wymienionych w tej specyfikacji.
4.	Oprogramowanie nie może przechowywać danych o deduplikacji w centralnej bazie. Utrata bazy danych używanej przez oprogramowanie nie może prowadzić do utraty możliwości odtworzenia backupu. Metadane deduplikacji muszą być przechowywane w plikach backupu.
5.	Oprogramowanie musi zapewniać warstwę abstrakcji nad poszczególnymi urządzeniami pamięci masowej, pozwalając utworzyć jedną wirtualną pulę pamięci na kopie zapasowe. Wymagane jest wsparcie dla nieograniczonej liczby pamięci masowych to takiej puli.
6.	Oprogramowanie musi pozwalać na tworzenie repozytorium kopii zapasowych bezpośrednio na zasobach Microsoft Azure Blob, Google Cloud Storage, Amazon S3, Wasabi Cloud Storage oraz na innych kompatybilnych z S3 przestrzeniach obiektowych. Dodatkowo, oprogramowanie musi wspierać archiwizowanie tych danych do Microsoft Azure Archive Blob Storage oraz Amazon S3 Glacier.
7.	Oprogramowanie musi wspierać niezmienność kopii zapasowych na potrzeby ochrony przed ransomware poprzez niedopuszczenie do usunięcia lub modyfikacji kopii zapasowej w zadanym okresie czasu.
8.	Oprogramowanie nie może instalować żadnych stałych agentów wymagających wdrożenia czy upgradowania wewnątrz maszyny wirtualnej dla jakichkolwiek funkcjonalności backupu lub odtwarzania
9.	Oprogramowanie musi oferować portal samoobsługowy, umożliwiający odtwarzanie użytkownikom wirtualnych maszyn, obiektów MS Exchange i baz danych MS SQL, Oracle oraz PostgreSQL (w tym odtwarzanie point-in-time)
10.	Oprogramowanie musi zapewniać możliwość delegacji uprawnień do odtwarzania na portalu
11.	Oprogramowanie musi mieć możliwość integracji z innymi systemami poprzez wbudowane RESTful API
12.	Oprogramowanie musi mieć wbudowane mechanizmy backupu konfiguracji w celu prostego odtworzenia systemu po całkowitej reinstalacji
13.	Oprogramowanie musi mieć wbudowane mechanizmy szyfrowania zarówno plików z backupami jak i transmisji sieciowej. Włączenie szyfrowania nie może skutkować utratą jakiejkolwiek funkcjonalności wymienionej w tej specyfikacji
14.	Oprogramowanie musi posiadać mechanizmy chroniące przed utratą hasła szyfrowania

15.	Oprogramowanie musi posiadać architekturę klient/serwer z możliwością instalacji wielu instancji konsoli administracyjnych.
16.	Oprogramowanie musi posiadać natywne mechanizmy uwierzytelniania wieloskładnikowego (MFA) w celu dostępu do konsoli administracyjnej
III. Wymagania RPO	
1.	Oprogramowanie musi wykorzystywać mechanizmy Change Block Tracking na wszystkich wspieranych platformach wirtualizacyjnych. Mechanizmy muszą być certyfikowane przez dostawcę platformy wirtualizacyjnej
2.	Oprogramowanie musi wykorzystywać mechanizmy śledzenia zmienionych plików przy zabezpieczaniu udziałów plikowych.
3.	Oprogramowanie musi oferować możliwość sterowania obciążeniem storage'u produkcyjnego tak aby nie przekraczane były skonfigurowane przez administratora backupu poziomy latencji. Funkcjonalność ta musi być dostępna na wszystkich wspieranych platformach wirtualizacyjnych z dokładnością do pojedynczego datastoru
4.	Oprogramowanie musi zapewniać tworzenie kopii zapasowych z bezpośrednim wykorzystaniem snapshotów macierzowych. Musi też zapewniać odtwarzanie maszyn wirtualnych z takich snapshotów. Proces wykonania kopii zapasowej nie może wymagać użycia jakichkolwiek hostów tymczasowych. Opisana funkcjonalność powinna działać w środowisku VMware.
5.	Oprogramowanie musi posiadać wsparcie dla VMware vSAN potwierdzone odpowiednią certyfikacją VMware.
6.	Oprogramowanie musi wspierać kopiowanie backupów oraz zasobów plikowych na taśmy.
7.	Oprogramowanie musi mieć możliwość tworzenia retencji GFS (Grandfather-Father-Son)
8.	Oprogramowanie musi wspierać bezpośrednią integrację z urządzeniami deduplikacyjnymi. Minimalnie wsparcie wymagane dla Dell DataDomain, HPE StoreOnce, ExaGrid, Fujitsu CS800, Quantum DXi oraz Infinidat InfiniGuard.
9.	Oprogramowanie musi wspierać BlockClone API w przypadku użycia Windows Server 2016, 2019 lub 2022 z systemem pliku ReFS jako repozytorium backupu. Podobna funkcjonalność musi być zapewniona dla repozytoriów opartych o linuxowy system plików XFS.
10.	Oprogramowanie musi mieć możliwość kopiowania backupów oraz replikacji wirtualnych maszyn z wykorzystaniem wbudowanej akceleracji WAN.
11.	Oprogramowanie musi mieć możliwość replikacji asynchronicznej włączonych wirtualnych maszyn bezpośrednio z infrastruktury VMware vSphere pomiędzy hostami

	ESXi oraz pomiędzy hostami Hyper-V. Dodatkowo oprogramowanie musi mieć możliwość użycia plików kopii zapasowych jako źródła replikacji.
12.	Oprogramowanie musi mieć możliwość replikacji ciągłej, opartej o VMware VAIO, włączonych wirtualnych maszyn bezpośrednio z infrastruktury VMware vSphere. Dla replikacji ciągłej musi być możliwość zdefiniowania dziennika pozwalającego na odzyskanie danych z dowolnego punku w ramach ustalonego parametru RPO.
13.	Oprogramowanie musi umożliwiać przechowywanie punktów przywracania dla replik
14.	Oprogramowanie musi umożliwiać wykorzystanie istniejących w infrastrukturze wirtualnych maszyn jako źródła do dalszej replikacji (replica seeding)
15.	Oprogramowanie musi wykorzystywać wszystkie oferowane przez hypervisor tryby transportu (sieć, hot-add, LAN Free-SAN)
IV. Wymagania RTO	
1.	Oprogramowanie musi umożliwiać jednoczesne uruchomienie wielu maszyn wirtualnych bezpośrednio ze zdeduplikowanego i skompresowanego pliku backupu, z dowolnego punktu przywracania, bez potrzeby kopiowania jej na storage produkcyjny. Funkcjonalność musi być oferowana dla środowisk VMware, Hyper-V oraz Nutanix AHV niezależnie od rodzaju storage'u użytego do przechowywania kopii zapasowych.
2.	Dodatkowo dla środowiska vSphere, Hyper-V i Nutanix AHV powyższa funkcjonalność powinna umożliwiać uruchomianie backupu z innych platform (inne wirtualizatory, maszyny fizyczne oraz chmura publiczna)
3.	Oprogramowanie musi pozwalać na migrację on-line tak uruchomionych maszyn na storage produkcyjny. Migracja powinna odbywać się mechanizmami wbudowanymi w hypervisor. Jeżeli licencja na hypervisor nie posiada takich funkcjonalności - oprogramowanie musi realizować taką migrację swoimi mechanizmami
4.	Oprogramowanie musi pozwalać na zaprezentowanie pojedynczego dysku bezpośrednio z kopii zapasowej do wybranej działającej maszyny wirtualnej vSpehre
5.	Oprogramowanie musi pozwalać na uruchomienie zasobów plikowych SMB oraz baz danych MS SQL i Oracle bezpośrednio ze skompresowanego i skompresowanego pliku backupu. Dodatkowo wspierana musi być migracja on-line tak uruchomionych zasobów na środowisko produkcyjne.
6.	Oprogramowanie musi umożliwiać pełne odtworzenie wirtualnej maszyny, plików konfiguracji i dysków
7.	Oprogramowanie musi umożliwiać pełne odtworzenie wirtualnej maszyny bezpośrednio do Microsoft Azure, Microsoft Azure Stack, Amazon EC2 oraz Google Cloud Platform.

I-I.271.11.2024 Gorzyce, 15.07.2024 r.

8.	Oprogramowanie musi umożliwić odtworzenie plików/folderów lub ich uprawnień na maszynę operatora, lub na serwer produkcyjny bez potrzeby użycia agenta instalowanego wewnątrz wirtualnej maszyny. Funkcjonalność ta nie powinna być ograniczona wielkością i liczbą przywracanych plików
9.	Oprogramowanie musi mieć możliwość odtworzenia plików bezpośrednio do maszyny wirtualnej poprzez sieć, przy pomocy natywnego API dla platformy VMware i PowerShell Direct dla platformy Hyper-V.
10.	Oprogramowanie musi wspierać odtwarzanie pojedynczych plików z systemów Windows, Linux, BSD, Solaris, Mac, Novell
11.	Oprogramowanie musi wspierać przywracanie plików z partycji Linux LVM
12.	Oprogramowanie musi umożliwiać szybkie granularne odtwarzanie obiektów aplikacji bez użycia jakiegokolwiek agenta zainstalowanego wewnątrz maszyny wirtualnej.
13.	Oprogramowanie musi wspierać granularne odtwarzanie obiektów Active Directory takich jak konta komputerów, konta użytkowników, dowolnych atrybutów, rekordów DNS zintegrowanych z AD, Microsoft System Objects, certyfikatów CA, elementów AD Sites oraz pozwalać na odtworzenie haseł.
14.	Oprogramowanie musi wspierać granularne odtwarzanie Microsoft Exchange 2013SP1 i nowszych (dowolny obiekt w tym obiekty w folderze "Permanently Deleted Objects"). Odtwarzanie musi być możliwe bezpośrednio do środowiska produkcyjnego.
15.	Oprogramowanie musi wspierać granularne odtwarzanie Microsoft SQL 2008 i nowszych. Odtwarzanie musi być możliwe bezpośrednio do środowiska produkcyjnego dla odzysku point-in-time, całych baz lub pojedynczych tabeli, widoków oraz procedur.
16.	Oprogramowanie musi wspierać granularne odtwarzanie Microsoft Sharepoint 2013 i nowszych. Odtwarzanie musi być możliwe bezpośrednio do środowiska produkcyjnego dla odzysku całych witryn, bibliotek oraz pojedynczych dokumentów wraz z historią ich wersji.
17.	Oprogramowanie musi wspierać granularne odtwarzanie baz danych Oracle z opcją odtwarzanie point-in-time wraz z włączonym Oracle DataGuard. Funkcjonalność ta musi być dostępna dla baz uruchomionych w środowiskach Windows oraz Linux.
18.	Oprogramowanie musi wspierać granularne odtwarzanie baz danych PostgreSQL z opcją odtwarzanie point-in-time. Funkcjonalność ta musi być dostępna dla baz uruchomionych w środowiskach Linux.
19.	Oprogramowanie musi posiadać natywną integrację dla backupów wykonywanych poprzez Oracle RMAN
20.	Oprogramowanie musi posiadać natywną integrację dla backupów wykonywanych poprzez SAP HANA, SAP Oracle

21.	Oprogramowanie musi posiadać natywną integrację dla backupów wykonywanych poprzez MS SQL VDI
22.	Oprogramowanie musi wspierać także specyficzne metody odtwarzania w tym "reverse CBT" oraz odtwarzanie z wykorzystaniem sieci SAN
V. Ograniczenie ryzyka	
1.	Oprogramowanie musi dawać możliwość stworzenia laboratorium (izolowane środowisko) dla vSphere i Hyper-V używając wirtualnych maszyn uruchamianych bezpośrednio z plików backupu. Powyższa funkcjonalność powinna umożliwiać uruchomianie backupu z innych platform (inne wirtualizatory, maszyny fizyczne oraz chmura publiczna)
2.	Dla VMware'a oprogramowanie musi pozwalać na uruchomienie takiego środowiska dla replik maszyn wirtualnych oraz bezpośrednio ze snapshotów macierzowych stworzonych na wspieranych urządzeniach.
3.	Oprogramowanie musi umożliwiać weryfikację odtwarzalności wielu wirtualnych maszyn jednocześnie z dowolnego backupu według własnego harmonogramu w izolowanym środowisku. Testy powinny uwzględniać możliwość uruchomienia dowolnego skryptu testującego również aplikację uruchomioną na wirtualnej maszynie. Testy muszą być przeprowadzone bez interakcji z administratorem
4.	Oprogramowanie musi umożliwiać integrację z oprogramowaniem antywirusowym w celu wykonania skanu zawartości pliku backupowego przed odtworzeniem jakichkolwiek danych. Integracja musi być zapewniona minimalnie dla Windows Defender, Symantec Protection Engine oraz ESET NOD32.
5.	Oprogramowanie musi umożliwiać dwuetapowe, automatyczne, odtwarzanie maszyn wirtualnych z możliwością wstrzyknięcia dowolnego skryptu przed odtworzeniem danych do środowiska produkcyjnego.
VI. Środowiska fizyczne	
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 system operacyjny macOS

I-I.271.11.2024 Gorzyce, 15.07.2024 r.

5.	Oprogramowanie musi wspierać odtwarzanie pojedynczych plików z systemów Windows, Linux, MacOS, Unix
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 zasobach 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, bezpośrednio na zasobach obiektowych (w tym 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 kopii zapasowych. Dla systemów Windows technologia śledzenia bloków dla systemów serwerowych musi być certyfikowana przez Microsoft
17.	Rozwiązanie musi wspierać technologię BitLocker
18.	Rozwiązanie musi wspierać uruchamianie z nośnika odtwarzania
19.	Rozwiązanie musi wspierać odzysk pojedynczych elementów aplikacji z jednoprzebiegowej kopii zapasowej dla Microsoft Exchange 2013SP1 i nowszych,

	Microsoft Active Directory 2008 i nowszych, Microsoft Sharepoint 2013 i nowszych, Microsoft SQL 2008 i nowszych, Oracle 11g i nowszych oraz PostgreSQL 12 i nowszych
20.	Rozwiązanie musi wspierać odzysk do konkretnego punktu w czasie (point-in-time) dla wspieranych systemów bazodanowych
21.	Rozwiązanie musi umożliwiać natychmiastowe publikowanie baz MS SQL i Oracle poprzez bezpośrednie uruchomienie ich z pliku backupu.
22.	Rozwiązanie musi wspierać odzysk obrazów kopii zapasowych bezpośrednio do vSphere, Hyper-V, Nutanix AHV, Microsoft Azure, Microsoft Azure Stack, Amazon EC2 oraz Google Cloud Platform
23.	Rozwiązanie musi wspierać szyfrowanie
24.	Rozwiązanie musi wspierać możliwość wykonywania kopii zapasowych stacji klienckich, lokalnie do repozytorium tymczasowego (cache) gdy połączenie sieciowe do głównego repozytorium kopii zapasowych jest niedostępne
25.	Rozwiązanie musi posiadać funkcjonalność automatycznego zmniejszenia szybkości przetwarzania danych, aby nie dopuścić do obniżenia wydajności systemu zabezpieczanego
26.	Rozwiązanie musi posiadać ochronę przed ransomware poprzez automatyczne odmontowanie nośnika po wykonanym backupie stacji klienckiej
27.	Rozwiązanie musi wspierać tworzenie wielu zadań backupowych
VII. 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 6.x, 7.x oraz 8.0 – 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 2012, 2012R2, 2016, 2019 oraz 2022 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 umożliwiać kategoryzacje obiektów infrastruktury wirtualnej niezależnie od hierarchii stworzonej w vCenter

I-I.271.11.2024 Gorzyce, 15.07.2024 r.

5.	System musi umożliwiać tworzenie alarmów dla całych grup wirtualnych maszyn jak i pojedynczych wirtualnych maszyn
6.	System musi dawać możliwość układania terminarza raportów i wysyłania tych raportów przy pomocy poczty elektronicznej w formacie HTML oraz Excel
7.	System musi dawać możliwość podłączenia się do kilku instancji vCenter Server i serwerów Hyper-V jednocześnie, w celu centralnego monitorowania wielu środowisk
8.	System musi mieć wbudowane predefiniowane zestawy alarmów wraz z możliwością tworzenia własnych alarmów i zdarzeń przez administratora
9.	System musi mieć wbudowane połączenie z bazą wiedzy opisującą problemy z predefiniowanych alarmów
10.	System musi mieć centralną konsolę z sumarycznym podglądem wszystkich obiektów infrastruktury wirtualnej (ang. Dashboard)
11.	System musi mieć możliwość monitorowania platformy sprzętowej, na której jest zainstalowana infrastruktura wirtualna
12.	System musi zapewnić możliwość podłączenia się do wirtualnej maszyny (tryb konsoli) bezpośrednio z narzędzia monitorującego
13.	System musi mieć możliwość integracji z oprogramowaniem do tworzenia kopii zapasowych tego samego producenta
14.	System musi mieć możliwość monitorowania obciążenia serwerów backupowych, ilości zabezpieczanych danych oraz statusu zadań kopii zapasowych, replikacji oraz weryfikacji odzyskiwalności maszyn wirtualnych.
15.	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.
16.	System musi mieć możliwość granularnego monitorowania infrastruktury, zależnego od uprawnień nadanym użytkownikom dla platformy VMware
17.	System musi mieć możliwość monitorowania instancji VMware vCloud Director w wersji od 10.x do 10.4
VIII. Raportowanie	
1.	System musi umożliwiać raportowanie środowiska wirtualizacyjnego Vmware w wersji 6.x, 7.x oraz 8.0 – zarówno w bezpłatnej wersji ESXi jak i w pełnej wersji ESX/ESXi zarządzane przez konsole vCenter Server lub pracujące samodzielnie

I-I.271.11.2024 Gorzyce, 15.07.2024 r.

2.	System musi umożliwiać raportowanie środowiska wirtualizacyjnego Microsoft Hyper-V 2012, 2012R2, 2016, 2019 oraz 2022 zarówno w wersji darmowej jak i zawartej w płatnej licencji Microsoft Windows Server zarządzane poprzez System Center Virtual Machine Manager lub pracujące samodzielnie.
3.	System musi wspierać wiele instancji vCenter Server i Microsoft Hyper-V jednocześnie bez konieczności instalowania dodatkowych modułów.
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)

I-I.271.11.2024 Gorzyce, 15.07.2024 r.

17.	System musi mieć możliwość generowania personalizowanych raportów zawierających informacje z dowolnych predefiniowanych raportów w pojedynczym dokumencie

13. Usługa w chmurze obliczeniowej typu IaaS, SaaS, PaaS dotycząca bezpieczeństwa sieciowego.

Przedmiotem zamówienia jest specjalistyczna usługa odmiejscowienia biblioteki taśmowej wraz z serwerem Zamawiającego oraz dodatkowym osprzętem (dalej: Urządzenia) w serwerowni Wykonawcy z uwzględnieniem montażu oraz konfiguracji krytycznych kopii zapasowych, okresie nie krótszym niż 24 miesięcy. Usługa obejmuje:

- udostępnienie niezbędnej przestrzeni, w tym RACK dla 2 dla Urządzeń o wysokości 1U, pozwalającej na prawidłowe wykonywanie krytycznych kopii zapasowych Zamawiającego, zgodnie z przyjętą polityką bezpieczeństwa, zwłaszcza w zakresie realizacji kopii zapasowych;
- zapewnienie redundantnego zasilania elektrycznego o określonej mocy, niezbędnej do prawidłowego działania Urządzeń, pozwalającego na zachowanie ciągłości działania w zakresie dystrybucji energii elektrycznej;
- zapewnienie redundantnego łącza internetowego, włączając w to co najmniej dwa niezależne przyłącza światłowodowe do serwerowni;
- zapewnienie gwarantowanego łącza internetowego z SLA o przepustowości symetrycznej co najmniej 500/500 Mbps, zapewniającego czas reakcji na awarie nie krótszy niż 2h oraz czas usunięcia awarii nie krótszy niż 8h;
- zapewnienie odpowiednich warunków temperaturowych i wilgotnościowych dla taśm magnetycznych przez cały czas trwania usługi;
- zapewnienie redundancji klimatyzacji w ilości co najmniej 4 niezależnie działających klimatyzatorów,

z niezależnym i autonomicznym źródłem zasilania pozwalającym na co najmniej sześciogodzinną pracę klimatyzacji w przypadku awarii zasilania;
- zapewnienie ochrony przeciwpożarowej z systemem gaszenia gazem HFC 227ea oraz systemem oddymiania pomieszczenia, w którym zlokalizowane zostaną Urządzenia;
- zapewnienie zasilania awaryjnego złożonego z urządzeń typu UPS oraz agregat prądotwórczy, zapewniającego podtrzymanie zasilania przez okres nie krótszy niż 6 godzin;
- zapewnienie bezpieczeństwa fizycznego Urządzeń, w tym co najmniej zapewnienie elektronicznego systemu kontroli dostępu do Urządzeń, całodobowej ochrony obiektu, monitoringu wizyjnego obiektu z przechowywaniem nagrań z serwerowni przez co najmniej 14 dni;
- serwisowanie infrastruktury serwerowni Wykonawcy, a w przypadku awarii Urządzeń, demontaż i wysyłka Urządzeń na adres wskazany przez Zamawiającego w celu wykonania serwisu naprawczego lub naprawy pogwarancyjnej;
- zapewnienie bezpiecznego szyfrowanego połączenia pomiędzy urządzeniami wskazanymi przez Zamawiającego, a Urządzeniami zlokalizowanymi w serwerowni Wykonawcy z wykorzystaniem urządzeń Wykonawcy po stronie Wykonawcy usługi;
- możliwość rozbudowy infrastruktury w przyszłości;
- brak możliwości dostępu do szafy, w której zlokalizowane są kopie zapasowe, osób innych niż pracownicy i współpracownicy Zamawiającego;
- zapewnienie możliwości korzystania z dodatkowych lokalnych usług serwisowych w zakresie obsługi Urządzeń.

14. Oprogramowanie do zarządzania i aktualizacji systemów operacyjnych i oprogramowania na stacjach roboczych, serwerach, urządzeniach sieciowych – 45 sztuk.

1. Podstawowe wymagania w zakresie oprogramowania do zarządzania i aktualizacji systemów operacyjnych na stacjach roboczych, serwerach, urządzeniach sieciowych oraz monitorowania infrastruktury informatycznej:

I-I.271.11.2024 Gorzyce, 15.07.2024 r.

- Dostarczone licencje na oprogramowanie są bezterminowe z dwu letnim wsparciem.
- Oprogramowanie musi posiadać procedurę uwierzytelnienia i autoryzacji Administratora w konsoli zarządzającej, który umożliwia jednoczesną prace wielu administratorom. Logowanie użytkowników konsoli zarządzającej powinno być zintegrowane z kontami Active Directory.
- Oprogramowanie współpracuje z serwerem SQL Server 2019, SQL Server 2017, SQL Server 2016 SP3, SQL Server 2014 SP3, Oracle 19c, Oracle 12c R2.
- Oprogramowanie serwera aplikacji umożliwia wysyłanie powiadomień mailowych.
- Oprogramowanie posiada system ról, dzięki któremu jest możliwe przypisywanie wybranych grup stanowisk do poszczególnych użytkowników konsoli.
- Wszelkie raporty, zestawienia oraz funkcje grupowe obejmują wtedy tylko w/w przypisane grupy stanowisk.
- Oprogramowanie realizuje zarządzanie wszystkimi modułami systemu z poziomu tej samej konsoli zarządzającej.
- Oprogramowanie agenta realizuje wszystkie wymagane funkcjonalności z poziomu jednej instancji usługi lub procesu bez wykorzystywania aplikacji oraz usług firm trzecich za wyjątkiem aplikacji oraz usług wbudowanych w system operacyjny na którym zainstalowany został Agent.
- Oprogramowanie pozwala export do plików w formacie xls/xlsx dowolnego widoku konsoli administracyjnej.
- Oprogramowanie pozwala zarządzać z jednej konsoli zarówno stacjami klienckimi, serwerami jak i urządzeniami mobilnymi z systemami operacyjnymi Android oraz iOS.
- Oprogramowanie, niezależnie od ilości funkcjonalności lub zarządzanych urządzeń końcowych działa w oparciu o 1 oprogramowanie typu Agent na urządzeniu końcowym.
- Oprogramowanie posiada architekturę trójwarstwową składającą się z Bazy Danych, Serwera Aplikacji oraz Agenta.
- Oprogramowanie działa poprawnie na wymaganiach sprzętowych:

Wymagania dla serwera:
- procesor 2 rdzenie;
- 8 GB wolnej pamięci;
- karta sieciowa 1 Gigabit;
- przestrzeń instalacyjna: 5 GB;
- Serwer OS - od Windows Server 2016 (64-Bit);
- Baza Danych - od SQL Server 2014 SP3;

Wymagania dla stacji klienckiej:
- od Intel Pentium IV procesor z 1GHz;
- od 256 MB wolnej pamięci RAM;
- od 200 MB wolnego miejsca na dysku twardym;

- Oprogramowanie musi posiadać procedurę uwierzytelnienia i autoryzacji Administratora w konsoli zarządzającej, który umożliwia jednoczesną prace wielu administratorom. Logowanie użytkowników konsoli zarządzającej powinno być zintegrowane z kontami Active Directory.
- Oprogramowanie umożliwia dystrybucję dowolnego oprogramowania, nie tylko paczek MSI, ale również takich jak InnoSetup, InstallShield i inne.
- Oprogramowanie umożliwia automatyzowanie instalatorów wraz z możliwością customizowania instalatorów w taki sposób, żeby można było nadpisywać pola opisowe, zmieniać dowolne wartości, w tym miejsce zapisu na dysku na urządzeniu końcowym.
- Oprogramowanie umożliwia administratorowi zautomatyzowanie procesu instalacji, w taki sposób, by nagrany został cały proces instalacji w taki sposób, by w momencie instalacji na urządzeniu końcowym nie było wymagane podanie jakichkolwiek opcji.

- Oprogramowanie musi umożliwiać zautomatyzowania zdalnej instalacji dowolnego oprogramowania w taki sposób, by oprogramowanie można było zainstalować zdalnie w trybie cichym (Silent Mode) lub graficznym.
- Oprogramowanie musi umożliwiać dodawanie takich opcji w instalatorach jak:

- blokowanie klawiatury i myszki;
- zmiany w ustawieniach w rejestracji na stacjach klienckich;
- działania na plikach I folderach na stacji klienckiej;
- dodanie skryptu np. w PowerShellu;
- zatrzymanie/wznowienie usług oraz procesów na stacji klienckiej.

- Zdalna dystrybucja oprogramowania musi wykorzystywać natywną inteligencję instalatora. Nie może wykorzystywać Snapshotingu.
- Zdalna dystrybucja oprogramowania musi mieć opcje Schedullingu:

- w zadanym przedziale czasowym;
- wprowadzenie cykliczności (np. wybrany dzień tygodnia o wybranej godzinie);
- połączenie dwóch powyższych;
- na żądanie w danym momencie;

- Oprogramowanie musi umożliwiać wzbudzanie stacji klienckich metodą Wake-On-LAN.
- Oprogramowanie musi umożliwiać administratorowi podgląd co do Statusu danego zadania per maszyna w czasie rzeczywistym, a w przypadku błędu w wykonaniu - zwrócić informację co było przyczyną błędu.
- W przypadku dokupienia nowych funkcjonalności/modułów oprogramowania, nie wymagana będzie jakakolwiek reinstalacja po stronie serwera (wystarczy podmiana klucza licencji oraz umożliwia aktualizację licencji online, bez konieczności wymiany plikowej).
- W przypadku zwiększenia ilości zarządzanych maszyn w dowolnym momencie, nie wymagana będzie jakakolwiek reinstalacja po stronie serwera (wystarczy podmiana klucza licencji oraz umożliwia aktualizację licencji online, bez konieczności wymiany plikowej).
- Oprogramowanie musi umożliwiać zdalną dystrybucję oprogramowania z jednej konsoli zarówno na stacjach klienckich (jak PC I laptop/notebook) jak i urządzeniach mobilnych z systemem Android.
- Oprogramowanie dostarczy administratorowi informacji o dacie ostatniego uruchomienia aplikacji na stacji klienckiej PC per każda stacja kliencka.
- Dystrybucja agentów na stacjach klienckich musi być możliwa zarówno w sposób automatyczny jak i ręczny.
- Oprogramowanie umożliwia integrację z Active Directory (AD) oraz pobranie informacji z AD i automatyczne zarejestrowanie urządzeń z AD w serwerze.
- Zarówno w przypadku stacji klienckich PC jak I urządzeń mobilnych z systemem Android, oprogramowanie musi umożliwiać administratorowi dostarczenie użytkownikowi końcowemu interfejsu typu self-service, w którym będzie miał listę dostępnych instalatorów z możliwością ich dociągnięcia i zainstalowania; Musi istnieć możliwość automatycznej personalizacji takiej listy per grupa lub konkretne urządzenie końcowe.
- Oprogramowanie musi posiadać otwarte API do integracji z zewnętrznymi serwerami, np. poprzez Web Service'y.
- Oprogramowanie musi umożliwiać również tworzenie własnych skryptów, które następnie można automatycznie instalować na urządzeniach końcowych, typu stacja kliencka.
- W przypadku automatycznej zdalnej instalacji oprogramowania na stacjach klienckich, oprogramowanie musi dać opcje tworzenia listy oprogramowania zależnego, tzn. w przypadku gdy do poprawnego działania aplikacja X wymaga instalacji aplikacji Y, Oprogramowanie musi dawać opcję ustalenia listy takiego oprogramowania zależnego na poziomie konfiguracji aplikacji X z poziomu konsoli. W przypadku dystrybucji aplikacji X, gdy na stacji klienckiej nie

będzie zainstalowana aplikacja Y, serwer automatycznie wypchnie na tą stację paczkę instalacyjną aplikacji Y.

- Oprogramowanie musi dawać administratorowi możliwość przypisywania wykonywania zadań zarówno na urządzeniach końcowych spełniających wybrane warunki dynamiczne (np. wolne miejsce na dysku C, wersja systemu operacyjnego itp.), jak i urządzeniach przypisanych do konkretnych grup, jak w AD.
- Oprogramowanie musi posiadać środowisko skryptowe, umożliwiające tworzenie własnych skryptów i w łatwej dystrybucji skryptów z poziomu konsoli.
- Oprogramowanie wspiera MsSQL-Server (również w wersji Express).
- Oprogramowanie posiada konsolę zarządzającą jako część oprogramowania (nie tylko interfejs webowy).
- Oprogramowanie posiada Agenta dla systemów klienckich Windows od Windows oraz Windows Server.
- Oprogramowanie wspiera więcej niż jeden serwer-repozytorium (DIP-Server).
- Oprogramowanie wspiera PXE-Relay.
- Oprogramowanie wspiera WakeUp-Points.
- Oprogramowanie posiada możliwość integracji z Active Directory.
- Oprogramowanie obsługuje niewielką przepustowością łącza dla kontroli agentów i przesyłania informacji o statusach.
- Oprogramowanie umożliwia indywidualną synchronizację pomiędzy pojedynczymi serwerami repozytorium (ograniczenie czasowe i przepustowości łącza).
- Oprogramowanie posiada dostęp read-only do AD, bez rozszerzeń schematu
- Oprogramowanie umożliwia wybudzanie stacji klienckich Wake-On-LAN.
- Oprogramowanie wspiera zadania/Joby Push i Pull (łącznie z Shutdown).
- Oprogramowanie umożliwia komunikację bez konieczności zestawiania połączenia VPN z urządzeniami, które są poza siecią poprzez bramkę Proxy instalowaną w DMZ. Bramka Proxy musi stanowić integralną część Oprogramowania. Komunikacja pomiędzy bramką a agentem, jak i bramką a serwerem musi odbywać się poprzez HTTPS.
- Oprogramowanie obsługuje niewielką przepustowością łącza dla kontroli agentów i przesyłania informacji o statusach.
- Oprogramowanie umożliwia indywidualną synchronizację pomiędzy pojedynczymi serwerami repozytorium (ograniczenie czasowe i przepustowości łącza).
- Oprogramowanie posiada dostęp read-only do AD, bez rozszerzeń schematu
- Oprogramowanie umożliwia wybudzanie stacji klienckich Wake-On-LAN.
- Oprogramowanie wspiera zadania/Joby Push i Pull (łącznie z Shutdown).
- Oprogramowanie umożliwia komunikację bez konieczności zestawiania połączenia VPN z urządzeniami, które są poza siecią poprzez bramkę Proxy instalowaną w DMZ. Bramka Proxy musi stanowić integralną część Oprogramowania. Komunikacja pomiędzy bramką a agentem, jak i bramką a serwerem musi odbywać się poprzez HTTPS.
- Oprogramowanie umożliwia wysyłanie polecenia w trybie "Push".
- Oprogramowanie umożliwia wysyłanie polecenia w trybie "Pull".
- Oprogramowanie umożliwia wysyłanie polecenia w trybie "shutdown".
- Oprogramowanie pozwala na indywidualną interakcję użytkownika w trakcie wykonywania zadania uruchomionego przez administratora w trybach: opóźnienie, odmowa, przypomnienie o instalacji.
- Oprogramowanie umożliwia wysyłanie polecenia Wake-on LAN.
- Oprogramowanie umożliwia automatyczne generowanie i wysyłanie powtarzających się zadań (recurring Jobs).

- Oprogramowanie umożliwia uruchomienie zadania z poziomu użytkownika końcowego poprzez Kiosk samoobsługowy SelfService (dostępny przez Web).
- Zadania mogą być inicjowane z poziomu aplikacji selfservice - konsoli Webowej.
- Zawartość aplikacji SelfService (Kiosku) może być definiowana zarówno per User/Grupa Userów jak i per PC/Organisation Unit.
- Oprogramowanie umożliwia dystrybucji patchy Windows bez WSUS.
- Oprogramowanie umożliwia triggerowanie z poziomu WSUS.
- Oprogramowanie umożliwia obsługę systemów operacyjne Microsoft — Windows Server 2008, Windows 7, Windows 8, Windows 10, Windows 11, Windows Server 2008R2, Windows Server 2012, Windows Server 2019 z natywną instalacją.
- Producent oprogramowania zapewnia stały dostęp do bazy danych z poprawkami Microsoft - baza jest dostępna dla Klienta z poziomu konsoli oprogramowania w dniu jej opublikowania przez Microsoft.
- Oprogramowanie umożliwia określenie ścisłych wymagań czasowych dla instalacji poprawek Microsoft i te wymagania kontrolować. Oprogramowanie nie wymaga ingerencji w reguły eksploatacji serwerów, a mimo to zapewnia ich odpowiednio szybkie zamknięcie w razie luk w zabezpieczeniach.
- Oprogramowanie pozwala administratorowi zarządzać aktualizacją systemów: możliwość sprawdzania tylko pod kątem brakujących poprawek i czy poprawki mają być od razu instalowane. Poprawki mogą być zatwierdzane automatycznie lub ręcznie. Oprogramowanie pozwala także ustalać reguły dla różnych grup w systemie IT.
- Oprogramowania pozwala by metodą drag and drop w środowisku zgodnym z MMC określać, w jakich systemach mają być instalowane poprawki. W taki sam sposób definiowane są również automatyczne instalacje i sytuacje, w których administrator ma być wcześniej pytany o zgodę. Oprogramowanie automatycznie pobiera wszystkie poprawki Microsoft i na żądanie automatycznie je rozprowadza w infrastrukturze Klienta zgodnie z wytycznymi administratora kreator skryptów, konfiguracji pakietów i autmatyzacja dowolnych procesów / Automate i Package Studio.
- Oprogramowanie pozwala na tworzenie plików transformacji (MST), które umożliwiają niezawodne dopasowanie do każdego MSI.
- Oprogramowanie pozwala na tworzenie kreatora instalacji dla dowolnej aplikacji - nie wymaga paczki MSI.
- Oprogramowanie pozwala tworzyć pakiety instalacyjne, gdzie w ramach procesu można zainstalować "n" aplikacji lub wykonać szereg dodatkowych funkcji związanych np. z inwentaryzacją.
- Oprogramowanie obsługuje wszystkie powszechnie dostępne na rynku systemy operacyjne Microsoft - Windows Vista i Server 2008, Windows 7, Windows 8, Windows10, Windows 11, Windows Server 2008R2, Windows Server 2012 i Windows 2019.
- Oprogramowanie umożliwia tworzenie plików sterujących (transform).
- Oprogramowanie pozwala na automatyzacje niemal każdego procesu wykonywanego ręcznie na komputerze.
- Oprogramowania pozwala na proste tworzenie skryptów metodą drag and drop.
- Oprogramowanie zawiera standardowy zestaw poleceń.
- Oprogramowanie posiada możliwość sterowania również interfejsami niezgodnymi ze standardem (np. Java).
- Oprogramowanie posiada pomoc kontekstową.
- Oprogramowanie posiada tryb testowy step by step.

2. Szczegółowe wymagania w zakresie oprogramowania do zarządzania i aktualizacji systemów operacyjnych na stacjach roboczych, serwerach, urządzeniach sieciowych oraz monitorowania infrastruktury informatycznej:

- Monitorowanie zużycia energii przez urządzenia w sieci.
- Generowanie raportów o zużyciu energii.
- Automatyczne wykrywanie i identyfikacja oprogramowania zainstalowanego na urządzeniach.
- Gromadzenie szczegółowych informacji o oprogramowaniu, takich jak nazwa, wersja, wydawca, data instalacji i licencja.
- Możliwość ręcznego dodawania oprogramowania do inwentaryzacji.
- Aktualizacja informacji o oprogramowaniu w czasie rzeczywistym.
- Automatyczne wykrywanie i identyfikacja wszystkich urządzeń w sieci, w tym komputerów, serwerów, urządzeń mobilnych i urządzeń sieciowych.
- Gromadzenie szczegółowych informacji o urządzeniach, takich jak model, typ, system operacyjny, adres IP, konfiguracja sprzętu i oprogramowanie.
- Aktualizacja informacji o urządzeniach w czasie rzeczywistym.
- Możliwość udzielania zdalnej pomocy użytkownikom.
- Dostęp do pulpitu użytkownika w czasie rzeczywistym.
- Kontrola myszy i klawiatury.
- Skanowanie urządzeń w sieci w poszukiwaniu luk w zabezpieczeniach.
- Identyfikacja luk w zabezpieczeniach oprogramowania, systemów operacyjnych i konfiguracji urządzeń.
- Generowanie raportów o lukach w zabezpieczeniach.
- Możliwość śledzenia i monitorowania luk w zabezpieczeniach.
- Możliwość priorytetyzacji luk w zabezpieczeniach do naprawy.

15. Oprogramowanie przeciwdziałające wyciekowi danych – 45 sztuk.

Oprogramowanie na licencji wieczystej z dwu letnim wsparciem.

1. Pełne wsparcie dla stacji roboczych z systemami Windows 7/Windows 8.1/Windows 10/Windows 11.
2. Serwer administracyjny musi oferować możliwość instalacji na systemach Windows Server 2012
i nowszych.
3. Pomoc w programie (help) i dokumentacja do programu dostępna w języku angielskim.
4. Konsola administracyjna oraz komunikaty klienta muszą być w języku polskim.
5. Serwer administracyjny musi wspierać instalację w oparciu o bazę MS SQL.
6. Serwer administracyjny musi działać w architekturze serwer-klient, gdzie komunikacja serwera zarządzającego z klientem odbywa się przy pomocy agenta.
7. Konsola zarządzająca musi umożliwiać pobranie pliku instalacyjnego agenta.
8. Serwer administracyjny musi umożliwiać wykonanie instalacji/dezinstalacji zdalnej klienta na stacjach roboczych.
9. Reguły DLP muszą być egzekwowane również w przypadku braku połączenia między klientem, a serwerem zarządzającym.
10. W przypadku braku połączenia klienta z serwerem zarządzającym, klient musi mieć możliwość lokalnego przechowywania informacji oraz zebranych danych do czasu ponownego połączenia z serwerem administracyjnym.
11. Serwer administracyjny musi umożliwiać zarządzanie za pośrednictwem konsol.
12. Administrator musi posiadać możliwość zarządzania bazą danych poprzez określone zadania: kopia bazy danych, kopia oraz wyczyszczenie bazy danych, wyczyszczenie bazy danych. Administrator musi posiadać możliwość określenia wykonywania czasu związanego z wykonywaniem zadań na bazie danych. Zadania powinny być wykonywane co najmniej z interwałem: raz na tydzień, raz na dwa tygodnie, raz w miesiącu, raz na trzy miesiące.

13. Administrator musi mieć możliwość konfiguracji automatycznej konserwacji dla bazy danych. Jeżeli rozmiar bazy danych osiągnie skonfigurowany rozmiar, najstarsze informacje muszą być usunięte z bazy danych, w celu nie przekroczenia skonfigurowanego rozmiaru bazy.
14. Serwer administracyjny programu musi mieć możliwość automatycznego pobierania aktualizacji definicji kategoryzowania stron internetowych, aplikacji oraz rozszerzeń plików. Musi być możliwość wyłączenia automatycznego pobierania.
15. Administrator musi mieć możliwość tworzenia nowych kont administratorów w konsoli programu jak i ich usuwania oraz klonowania.
16. Administrator musi mieć możliwość przypisywania jak i odbierania uprawnień do wybranych modułów programu. Uprawnienia muszą być podzielone na:
a. Ustawienia, które określają możliwość wykonania konfiguracji na poszczególnym module,
b. Logi, które określają możliwość wyświetlenia logów poszczególnego modułu.
17. Serwer musi posiadać możliwość synchronizacji użytkowników oraz stacji roboczych z domeną Active Directory.
18. System musi posiadać możliwość logowania zdarzeń aktywności stacji roboczej, w oparciu o co najmniej:
a. logowanie oraz wylogowanie użytkownika,
b. włączenie oraz wyłączenie stacji roboczej,
c. blokada oraz odblokowanie stacji roboczej,
d. przejście w stan bezczynności stacji roboczej.
19. Administrator musi mieć możliwość, wymuszenia synchronizacji ustawień oraz logów, pomiędzy stacją roboczą, a serwerem, w czasie rzeczywistym.
20. Serwer administracyjny musi mieć możliwość ustawienia powiadomień dla użytkownika końcowego, w przypadku złamania reguł ustawionych w modułach związanymi z ochroną DLP. W powiadomieniu administrator musi posiadać możliwość określenia własnej grafiki, kontaktowego adresu e-mail oraz odnośnika do polityki bezpieczeństwa organizacji.
21. Oprogramowanie musi posiadać możliwości audytu stacji roboczych/użytkowników w oparciu o uruchomione aplikacje, podłączane urządzenia, odwiedzane strony internetowe, wydrukowane dokumenty, ruch sieciowy, wysyłane oraz odebrane wiadomości e-mail oraz wykonane czynności na plikach.
22. Administrator musi posiadać możliwość tworzenia własnych kategorii dla stron internetowych, aplikacji oraz typów plików.
23. Administrator musi posiadać możliwość filtrowania oraz sortowania zebranych danych. Tak odfiltrowane dane, administrator może zapisać w postaci plików PDF bądź XLS.
24. Konsola musi posiadać możliwość wysyłania powiadomień, jeśli dany użytkownik przekroczy określoną dopuszczalną ilość wysyłanych maili oraz w przypadku przekroczenia dopuszczalnej ilości wysyłanych danych do sieci w danym dniu lub tygodniu.
25. Serwer musi posiadać możliwość wysłania alertów, co najmniej za pośrednictwem wiadomości email.
26. Serwer administracyjny musi posiadać możliwość konfiguracji raportów w oparciu o uruchomione aplikacje, podłączane urządzenia, odwiedzane strony internetowe, drukowane dokumenty, ruch sieciowy, wysyłane wiadomości e-mail oraz wykonywane czynności na plikach.
27. Raporty muszą być generowane w oparciu o wskazane stacje robocze, użytkowników bądź grupy w określonym przedziale czasu.
28. Raporty muszą być generowane do pliku PDF i/lub XLS, po podaniu lokalizacji zapisywanego pliku lub na wskazany adres(y) e-mail.
29. Serwer administracyjny musi posiadać wbudowany serwer SMTP udostępniony przez producenta oprogramowania.
30. Serwer administracyjny musi umożliwiać kategoryzację (tagowanie) plików na poziomie systemu plików lub na poziomie metadanych pliku.

31. Serwer administracyjny musi umożliwiać wykonanie zadania kategoryzacji (tagowania) plików, które już znajdują się na stacjach roboczych i zasobach sieciowych, ale również nowych plików, które powstaną na bazie już skategoryzowanych (otagowanych) plików.
32. Serwer administracyjny musi mieć możliwość kategoryzacji (tagowania) plików wrażliwych w oparciu o:
a. aplikacje, z której zostały utworzone,
b. lokalizację,
c. adres URL,
d. format pliku,
e. zawartość pliku.
33. Administrator musi mieć możliwość wyszukiwania danych osobowych na zasobach zarówno lokalnych jak i sieciowych.
34. Dla plików skategoryzowanych (otagowanych), musi być możliwe utworzenie następujących reguł:
a. blokowanie oraz zezwalanie na zapisywanie, przenoszenie plików, do lokalizacji na określonych dyskach lokalnych,
b. blokowanie oraz zezwalanie na zapisywanie, przenoszenie do lokalizacji na dyskach zewnętrznych
z możliwością określenia białej oraz czarnej listy tych urządzeń,
c. blokowanie oraz zezwalanie na drukowanie na określonych drukarkach,
d. blokowanie oraz zezwalanie na zapisywanie i przenoszenie do lokalizacji sieciowej,
e. blokowanie oraz zezwalanie na wysyłanie za pośrednictwem klientów pocztowych z możliwością określenia białej i czarnej listy adresów i domen,
f. blokowanie oraz zezwalanie na wysyłanie do poczty webowej,
g. blokowanie oraz zezwalanie na zapisywanie, przenoszenie plików do chmury, zarówno za pomocą przeglądarki internetowej jak i aplikacji, w oparciu o co najmniej poniższe usługi:

- Dropbox,
- Google Drive,
- SharePoint,
- OneDrive Business,
- OneDrive Personal.
- blokowanie oraz zezwalanie na przesyłanie za pomocą komunikatorów,
- blokowanie oraz zezwalanie na zapisywanie i przenoszenie danych poprzez usługę pulpitu zdalnego,
- blokowanie oraz zezwalanie na wykonywanie zrzutów ekranowych, skopiowania zawartości oraz wirtualnego drukowania,
- uruchomienie wybranego formatu pliku przez wskazaną przez administratora aplikacje,

35. Serwer administracyjny musi umożliwiać możliwość zabezpieczenia korzystania z niezaufanych repozytoriów GIT.
36. Każda z polityk musi posiadać możliwość ustawienia jej w trybie powiadomienia dla użytkownika.
37. Serwer administracyjny musi dawać możliwość klasyfikacji pliku (tagowania) użytkownikowi na stacji roboczej. Klasyfikacja musi odbywać się poprzez integrację z menu kontekstowym.
38. Klasyfikacja użytkownika musi posiadać opcję, która uniemożliwi użytkownikowi zmianę klasyfikacji na niższą.
39. Serwer administracyjny musi umożliwiać określenie białych i czarnych list zawierających urządzenia pamięci masowej, drukarki fizycznych i sieciowych, lokalizacji sieciowych, adresów e-mail oraz domen, urządzeń przenośnych, firewire oraz bluetooth, które mogą być wykorzystywane do określenia reguł dostępu.

40. Serwer administracyjny musi posiadać funkcjonalność globalnego zablokowania lub zezwolenia na korzystanie z określonych folderów lokalnych, sieciowych, dysków o określonych literach oraz folderów synchronizacji z usługami chmury.
41. Serwer musi posiadać funkcjonalność skonfigurowania reguł dostępu dla urządzeń podłączanych do portu USB, urządzeń przenośnych, nośników optycznych CD/DVD, urządzeń Firewire, urządzeń podczerwieni, urządzeń Bluetooth, portów COM oraz LPT.
42. Serwer administracyjny musi posiadać możliwość zaszyfrowania całej powierzchni dysku w oparciu o funkcjonalność BitLocker z użyciem hasła lub modułu TPM.
43. Serwer administracyjny musi posiadać możliwość szyfrowania dysków zewnętrznych w oparciu o funkcjonalność BitLocker. Szyfrowanie oraz autoryzacja dla zaszyfrowanych nośników wymiennych musi być w pełni niezauważalna dla użytkownika.
44. Serwer administracyjny musi posiadać możliwość wyświetlenia i eksportu klucza odzyskiwania do zaszyfrowanych dysków oraz dysków wymiennych.
45. Serwer administracyjny musi posiadać możliwość wyszukiwania i ochrony plików w oparciu o ich zawartość, co najmniej o:
    a. numery kart kredytowych,
    b. numer PESEL,
    c. numer polskiego dowodu osobistego,
    d. polski numer paszportu,
    e. wyrażenia regularne,
    f. określone ciągi znaków,
    g. numer IBAN.
46. Weryfikacja zawartości pliku musi odbywać się w czasie rzeczywistym.
47. Weryfikacja zawartości pliku w czasie rzeczywistym musi posiadać funkcjonalność OCR (Optical Character Recognition).
48. System musi posiadać możliwość importu własnych słowników do wyszukiwania danych.
49. W przypadku incydentu bezpieczeństwa, system musi wykonać duplikat pliku lub wiadomości e- mail, w którym znajdują się dane wrażliwe (tzw. funkcjonalność „Shadow-copy").
50. Serwer administracyjny musi posiadać możliwość wyznaczenia progu ilości wystąpień danych wrażliwych, od jakich zostanie uruchomione zadanie klasyfikacji (tagowania).
51. Serwer administracyjny musi posiadać możliwość integracji klasyfikacji danych, z modułem DLP dostępnym na rozwiązaniu FortiGate.
52. Serwer administracyjny musi umożliwiać eksport logów do rozwiązania FortiSIEM.
53. Serwer administracyjny musi umożliwiać eksport identyfikatorów oznaczonych plików do rozwiązania FortiMail, które będzie w stanie kontrolować przesyłanie tak oznaczonych plików.
54. Serwer administracyjny musi umożliwiać integrację z Office365. Integracja musi pozwalać na:
    a. audyt i logowanie wiadomości e-mail,
    b. audyt i logowanie operacji na plikach,
    c. wprowadzanie polityk zabezpieczeń do wiadomości e-mail.
55. System musi umożliwiać integrację z narzędziami analitycznymi tj. Power BI, Tabeau).
56. Serwer administracyjny musi posiadać konsolę dostępną z poziomu przeglądarki internetowej, służącą do raportowania i zarządzania stacjami roboczymi i urządzeniami mobilnymi.
57. Konsola musi wyświetlać informacje na temat bezpieczeństwa danych, produktywności pracowników oraz utylizacji sprzętu które są podzielone na:
    a. Bezpieczeństwo danych:
    - Przegląd informacji o incydentach bezpieczeństwa.
    - Przegląd danych przychodzących.
    - Przegląd danych wychodzących.
    - Przegląd informacji z Office365 które dotyczą m.in. pobierania, współdzielenia oraz lokalnego dostępu do plików.

- Podłączane/odłączane urządzenia przenośne.

b. Produktywność:

- Przegląd informacji na temat produktywności użytkowników.
- Aktywność użytkowników podczas przeglądania stron WWW oraz korzystania z aplikacji.
- Trendy.

c. Eksploatacja sprzętu:

- Przegląd informacji na temat eksploatacji sprzętu komputerowego.
- Eksploatacja sprzętu komputerowego, najbardziej nieaktywne komputery.
- Eksploatacja drukarek.
- Eksploatacji sieci.

58. Konsola webowa musi posiadać możliwość konfiguracji/zmiany domyślnego serwera SMTP.
59. Konsola webowa musi umożliwiać weryfikację wersji zainstalowanego oprogramowania klienta wraz z możliwością aktualizacji do nowej wersji lub dezaktywacji tego oprogramowania.
60. Konsola webowa musi umożliwiać wygenerowanie raportu w postaci pliku DOCX, który zawiera informacje nt:

- plików przenoszonych na nośniki USB i inne urządzenia przenośne,
- plików przesłanych za pomocą wiadomości e-mail,
- plików przesłanych za pomocą poczty webowej,
- plików przesłanych do Internetu,
- plików wysłanych za pomocą komunikatorów,
- plików przesłanych na dyski chmurowe,
- analiza sposobu korzystania z aplikacji,
- analiza korzystania z Internetu,
- analiza wykorzystania porali do poszukiwania pracy.

16. Wdrożenie systemów teleinformatycznych.

Wdrożenie klastra serwerów

Krok 1: Planowanie i Przygotowanie

- Określenie wymagań dotyczących infrastruktury, w tym sprzętu, sieci i przechowywania.
- Wybranie serwerów, które zostaną użyte jako węzły klastra. Upewnij się, że są one zgodne z wymaganiami wybranego oprogramowania.
- Skonfigurowanie łącza sieciowego i przestrzeni dyskowej, aby zapewnić odpowiednią przepustowość i pojemność.
- Zainstalowanie systemu operacyjnego na każdym węźle klastra.

Krok 2: Instalacja roli oprogramowania do wirtualizacji

- Instalacja odpowiedniej roli za pomocą menedżera serwerów lub PowerShell.
- Konfiguracja ustawień sieciowych i przechowywania na węzłach klastra, tak aby były zgodne z wymaganiami projektu.

Krok 3: Konfiguracja klastra

- Uruchomienie kreatora konfiguracji klastra w menedżerze serwerów na jednym z węzłów.
- Dodanie pozostałych węzłów klastra do konfiguracji.
- Konfiguracja ustawień klastra, takie jak nazwa klastra, adresy IP i konfiguracja przechowywania współdzielonego.

Krok 4: Konfiguracja wysokiej dostępności klastra

- Włączenie funkcji wysokiej dostępności dla maszyn wirtualnych na klastrze.
- Konfiguracja ustawień zapasowych dla klastra, aby zapewnić ochronę przed awariami węzłów.

Krok 5: Tworzenie i Zarządzanie Maszynami Wirtualnymi

- Utworzenie nowych maszyn wirtualnych na klastrze z wykorzystaniem oprogramowania do wirtualizacji.

- Konfiguracja ustawień maszyn wirtualnych, takich jak liczba procesorów, ilość pamięci i przypisywanie zasobów sieciowych.
- Zarządzanie maszynami wirtualnymi, monitorowanie ich wydajności i wykonywanie niezbędnych operacji konserwacyjnych jest kluczowe w zapewnieniu prawidłowo funkcjonującego środowiska wirtualnego uruchomionego w klastrze.

Krok 6: Testowanie i Monitorowanie

- Testowanie działania klastra, w tym jego zdolność do migracji wirtualnej i przywracania po awariach.
- Konfiguracja narzędzi monitorujących, w celu śledzenia wydajności i dostępności klastra oraz maszyn wirtualnych.
- Regularnie przeglądanie logów i raportów, w celu szybkiego reagowania na ewentualne problemy.

17. Wdrożenie systemów teleinformatycznych.

Wdrożenie kontrolera domeny (AD)

Etap 1: Analiza Wstępna i Planowanie Wdrożenia

1.1. Analiza Stanu Obecnego:

- Ocena istniejącej infrastruktury IT, w tym systemów operacyjnych, sieci, aplikacji i baz danych.
- Identyfikacja istniejących rozwiązań zarządzania tożsamościami i bezpieczeństwem oraz ich ewentualnych ograniczeń.

1.2. Wymagania Organizacyjne i Techniczne:

- Konsultacje z interesariuszami w celu zrozumienia potrzeb biznesowych i oczekiwań dotyczących infrastruktury IT.
- Identyfikacja wymagań dotyczących zarządzania tożsamościami użytkowników, zasobami sieciowymi i politykami bezpieczeństwa.

1.3. Opracowanie Planu Wdrożenia:

- Sporządzenie szczegółowego planu projektowego uwzględniającego harmonogram, zadania, zasoby
i odpowiedzialności.
- Określenie struktury domen, schematu nazewnictwa i strategii replikacji dla środowiska Active Directory.

Etap 2: Instalacja i Konfiguracja Środowiska Active Directory

2.1. Instalacja Roli AD DS:

- Konfiguracja serwera Windows Server jako kontrolera domeny, włączając rolę Active Directory Domain Services.

2.2. Konfiguracja DNS:

- Ustawienie serwera DNS zgodnie z wymaganiami Active Directory.
- Konfiguracja strefy forward i reverse DNS dla domeny.

2.3. Tworzenie Dominy lub Integracja:

- Utworzenie nowej domeny Active Directory lub integracja z istniejącymi domenami w środowisku.

2.4. Konfiguracja Zasad Replikacji:

- Określenie i skonfigurowanie zasad replikacji między kontrolerami domeny w różnych lokalizacjach.

Etap 3: Strukturyzacja i Organizacja Domeny

3.1. Projektowanie Struktury Organizacyjnej:

- Tworzenie jednostek organizacyjnych (OU) odpowiadających strukturze organizacyjnej firmy.
- Utworzenie kont użytkowników, grup i zasobów oraz ich odpowiednie uporządkowanie w hierarchii.

3.2. Konfiguracja Polityk Grupowych (GPO):

- Ustanowienie zasad dostępu, konfiguracji użytkowników i komputerów za pomocą GPO.
- Implementacja polityk bezpieczeństwa dotyczących haseł, dostępu i innych ustawień

Etap 4: Zabezpieczenie Active Directory

4.1. Wdrożenie Zaawansowanych Mechanizmów Zabezpieczeń:

- Konfiguracja zasad kont haseł, polityk blokowania kont, kontroli dostępu.
- Implementacja szyfrowania komunikacji i audytu zdarzeń w AD.

4.2. Konfiguracja Środków Obronnych:

- Wdrożenie mechanizmów zabezpieczeń przed atakami, w tym monitorowanie logów, wykrywanie zagrożeń i zapobieganie atakom.

Etap 5: Walidacja i Optymalizacja Konfiguracji

5.1. Testowanie Funkcjonalności i Bezpieczeństwa:

- Przeprowadzenie testów weryfikujących działanie i bezpieczeństwo środowiska AD.
- Identyfikacja i rozwiązywanie ewentualnych problemów lub luk w zabezpieczeniach.

5.2. Optymalizacja Wydajności:

- Optymalizacja konfiguracji AD w celu zapewnienia efektywności i wydajności działania.
- Integracja z istniejącymi systemami i aplikacjami w celu zapewnienia spójności działań.

Etap 6: Dokumentacja Techniczna

6.1. Sporządzenie Dokumentacji:

- Przygotowanie szczegółowej dokumentacji technicznej, zawierającej opisy konfiguracji, ustawień polityk, procedur bezpieczeństwa i architektury systemu.
- Dokumentacja będzie służyć jako punkt odniesienia dla administratorów IT i personelu technicznego.

Cel Końcowy Usługi

Finalizacja usługi zapewni pełne wdrożenie systemu Active Directory, skonfigurowane zgodnie z najlepszymi praktykami branżowymi, gotowe do efektywnego zarządzania środowiskiem IT. System będzie przygotowany do zapewnienia wysokiego poziomu bezpieczeństwa, stabilności operacyjnej i skalowalności, odpowiadając na bieżące oraz przyszłe potrzeby organizacji.

18. Wdrożenie oprogramowania do wykonywania kopii zapasowych.

1: Planowanie i Przygotowanie

- Określenie wymagań dotyczących backupu i replikacji, w tym ilość danych do przechowywania, czas przywracania, dostępność i inne czynniki.
- Weryfikacja posiadania odpowiedniej ilości przestrzeni dyskowej i zasobów sieciowych do przechowywania kopii zapasowych.
- Pobranie niezbędnego oprogramowania do wykonywania kopii zapasowych i przeczytanie jego dokumentacji.

2: Instalacja i Konfiguracja

- Uruchomienie instalatora wybranego oprogramowania do wykonywania kopii zapasowych na wybranym serwerze.
- Postępuj zgodnie z kreatorami instalacji, akceptując licencję, wybierając komponenty do zainstalowania i konfigurując ustawienia.
- Konfiguracja połączenia ze swoim środowiskiem wirtualizacji

3: Konfiguracja Backupu

- Konfiguracja planów backupu, określając harmonogramy, miejsca przechowywania i inne parametry.
- Wybranie, które maszyny wirtualne lub inne zasoby będą chronione za pomocą kopii zapasowych.
- Ustawienie retencji danych i polityki przechowywania, aby dostosować je do wymagań firmy.

4: Konfiguracja Replikacji (opcjonalnie)

- Konfiguracje odpowiedniego zadania replikacji, określając maszyny wirtualne źródłowe i docelowe, harmonogramy i inne parametry.
- Weryfikacja dostępności docelowego środowiska na przyjęcie replikowanych maszyn wirtualnych.

5: Testowanie i Wdrażanie

- Przetestowanie planów backupu i replikacji, aby upewnić się, że są one zgodne z oczekiwaniami i spełniają wymagania czasu przywracania.
- Wdrożenie skonfigurowanych i przetestowanych planów na produkcji, monitorując ich wydajność
i skuteczność.

6: Monitorowanie i Administracja

- Regularne monitorowanie wykonywanych kopii zapasowych i replikacji, w celu weryfikacji ich poprawności i zgodności z planem.
- Weryfikacja raportów i dzienników zdarzeń oprogramowania do wykonywania kopii zapasowych, aby szybko reagować na jakiekolwiek problemy.

19. Wdrożenie systemów teleinformatycznych.

Dostawa i wdrożenie oprogramowania do monitorowania zasobów IT:
Wymagania w zakresie oprogramowania:

- Automatyczne odkrywanie sieci.
- Monitorowanie wydajności i dostępności.
- Zaawansowane wizualizacje danych, w tym wykresy, mapy i wykresy słupkowe.
- Wbudowane narzędzia do przetwarzania i analizy danych.
- Możliwość monitorowania przez SNMP, JMX, IPMI, agenta Zabbix i inne.
- Szeroka gama integracji z zewnętrznymi systemami.
- Elastyczność w konfiguracji elementów monitorowanych.
- Wsparcie dla monitorowania aplikacji, serwerów, sieci i urządzeń.
- Możliwość definiowania scenariuszy monitorowania.
- Rozbudowane opcje powiadomień i alarmów.
- Wsparcie dla skryptów i automatyzacji zadań.
- Monitorowanie transakcji biznesowych i aplikacji webowych.
- Wbudowane rozwiązania do diagnostyki i rozwiązywania problemów.
- Możliwość tworzenia niestandardowych wskaźników monitorowania.
- Skalowalność i możliwość monitorowania tysięcy urządzeń.
- Wsparcie dla monitorowania w chmurze i środowiskach wirtualnych.
- Zaawansowane raportowanie i analizy trendów.
- Integracja z systemami ticketowymi.
- Możliwość tworzenia dashboardów i paneli.
- Wsparcie dla różnorodnych systemów operacyjnych.
- Elastyczne opcje autentykacji i kontroli dostępu.
- Szyfrowanie komunikacji.
- Możliwość monitorowania baz danych.
- Wsparcie dla wysokiej dostępności i redundancji.
- Automatyczne odkrywanie urządzeń w sieci.
- Monitorowanie wykorzystania zasobów.
- Możliwość śledzenia zmian konfiguracyjnych.
- Integracja z rozwiązaniami do zarządzania konfiguracją.
- Możliwość zbierania danych z różnych źródeł.
- Wsparcie dla monitorowania środowisk kontenerowych.
- Możliwość definiowania zależności między monitorowanymi elementami.

- Zaawansowane filtrowanie i wyszukiwanie danych.
- Możliwość monitorowania poprzez proxy.
- Wsparcie dla niestandardowych skryptów monitorujących.
- Automatyczne wykrywanie problemów i anomalii.
- Możliwość grupowania urządzeń i aplikacji.
- Wsparcie dla monitorowania sieciowych urządzeń peryferyjnych.
- Możliwość tworzenia template'ów monitorowania.
- Wsparcie dla różnych metod zbierania danych (polling, trapper, SNMP traps).
- Możliwość tworzenia hierarchii monitorowania.
- Wsparcie dla wielojęzyczności interfejsu użytkownika.
- Możliwość zarządzania poprzez interfejs webowy.
- Zaawansowane opcje logowania i audytu.
- Wsparcie dla monitorowania poprzez protokół HTTPS.
- Możliwość definiowania zdarzeń i akcji.
- Możliwość monitorowania szyfrowanych połączeń.
- Integracja z systemami zarządzania logami.
- Wsparcie dla SNMP v3.
- Możliwość definiowania i monitorowania SLA.
- Wsparcie dla rozproszonego monitoringu.

Wymagania w zakresie wdrożenia oprogramowania:

Krok 1: Planowanie i Przygotowanie

- Określenie wymagań dotyczących monitorowania, obejmujące zarówno liczbę urządzeń, które będą monitorowane, jak i typy parametrów, których monitorowanie jest kluczowe dla działania infrastruktury IT. Dodatkowo, konieczne jest sprecyzowanie oczekiwanych powiadomień w przypadku wykrycia nieprawidłowości lub awarii.
- Dokonanie wyboru odpowiedniej platformy do instalacji narzędzia monitorującego, uwzględniając różnice między systemem operacyjnym Linux a Windows. W tym procesie istotne jest także przypisanie odpowiednich zasobów sprzętowych i sieciowych, aby zapewnić odpowiednią wydajność i dostępność narzędzia.
- Pobranie najnowszej wersji wybranego narzędzia do monitorowania zasobów IT oraz dokładnie zapoznaj się z dokumentacją. Zapoznanie się z dokumentacją pozwoli na lepsze zrozumienie funkcjonalności narzędzia oraz prawidłową konfigurację i wykorzystanie jego możliwości w procesie monitorowania infrastruktury IT.

Krok 2: Instalacja i Konfiguracja serwera (procesu centralnego) narzędzia do monitorowania zasobów IT

- Przeprowadzenie instalacji serwera, który pełni rolę centralnego procesu narzędzia do monitorowania zasobów IT. Począwszy od wybranej platformy, postępujemy zgodnie z precyzyjnie określonymi instrukcjami instalacyjnymi, które są dostępne w dokumentacji danego rozwiązania.
- Konfiguracja centralnego procesu narzędzia. W ramach konfiguracji, należy zapewnić odpowiedni dostęp do bazy danych. Możesz użyć różne systemy zarządzania bazami danych, takie jak MySQL, PostgreSQL lub SQLite.
- Ustalenie parametrów monitorowania, które obejmują specyficzne aspekty środowiska IT podlegające monitorowaniu. Dodatkowo, konieczne jest skonfigurowanie powiadomień, aby zapewnić odpowiednie reakcje na wykryte nieprawidłowości czy awarie. Poprzez precyzyjne skonfigurowanie tych ustawień, można efektywnie zarządzać monitorowanymi zasobami IT oraz szybko reagować na wszelkie pojawiające się problemy.

Krok 3: Instalacja i Konfiguracja Agentów wybranego narzędzia na Monitorowanych Hostach

- Instalacja agentów na wszystkich urządzeniach, które podlegają monitorowaniu, obejmując serwery, routery, przełączniki oraz inne istotne elementy infrastruktury IT.
- Konfiguracja agentów, aby komunikowały się z wcześniej zainstalowanym i skonfigurowanym serwerem.

- Określenie parametrów komunikacji, takich jak adres serwera monitorującego oraz porty, aby umożliwić płynną wymianę danych pomiędzy agentami a serwerem.

Krok 4: Konfiguracja Monitorowanych Parametrów i Wykresów

- Konfiguracja elementów monitorowania, takich jak elementy, wykresy, triggery i akcje, aby monitorować ważne parametry systemowe i aplikacyjne. Umożliwi to kompleksowe śledzenie wybranych parametrów, takich jak obciążenie CPU, zużycie pamięci, dostępność usług, wydajność aplikacji.
- Dostosowanie progów alarmowych dla trigerów, w celu uzyskania optymalnych powiadomień o ewentualnych awariach lub nieprawidłowościach w działaniu systemu. Warto zadbać o precyzyjne ustalenie progów alarmowych, aby uniknąć fałszywych alarmów oraz zapewnić skuteczną ochronę środowiska IT.

Krok 5: Testowanie i Optymalizacja

- Weryfikacja skonfigurowanych monitorów i triggerów, aby upewnić się, że działają zgodnie z oczekiwaniami. Testowanie powinno obejmować różne scenariusze działania systemu, aby zweryfikować skuteczność monitorowania w różnych warunkach. Poprawne działanie monitorów i trigerów jest kluczowe dla zapewnienia szybkiej reakcji na ewentualne problemy.
- Optymalizacja konfiguracji narzędzia do monitorowania zasobów IT, w celu zapewnienia wydajności
i skuteczności monitorowania, np. poprzez dostosowanie interwałów sprawdzania.

Krok 6: Monitorowanie i Administracja

- Regularne monitorowanie stanu urządzeń i aplikacji za pomocą interfejsu narzędzia do monitorowania zasobów IT pozwoli szybko identyfikować ewentualne zagrożenia lub nieprawidłowości w działaniu systemu, co umożliwia szybką reakcję i zapobieganie poważnym problemom.
- Reagowanie na alarmy i zdarzenia, które występują w środowisku monitorowanym.
W przypadku pojawiających się alarmów i zdarzeń, podejmować niezbędne działania naprawcze w celu przywrócenia normalnego funkcjonowania systemu.
- Regularne aktualizowanie oprogramowania do monitorowania zasobów IT, zapewni dostęp do najnowszych funkcji i poprawek bezpieczeństwa, co jest kluczowe dla utrzymania wysokiej jakości monitorowania oraz zapewnienia zgodności z aktualnymi standardami i wymaganiami branżowymi.

20. Wdrożenie SIEM.

Zamawiający na potrzeby wdrożenia udostępni infrastrukturę na serwerach zwirtualizowanych, wg. specyfikacji uzgodnionych z Wykonawcą. Czynności związane z wdrożeniem systemu będącego przedmiotem umowy będzie wykonywał Wykonawca. Instalacja systemu przez Wykonawcę odbywać się będzie z wykorzystaniem środków komunikacji elektronicznej.

1. Funkcjonalności systemu.
    1. Monitorowanie występujących zdarzeń (logów) w trybie ciągłym.
    2. Zbieranie zdarzeń z serwerów wirtualnych, fizycznych, Active Directory, przełączników oraz innego rodzaju urządzeń, które są oraz zostaną podłączone do infrastruktury zamawiającego.
    3. Agregacja oraz korelacja logów.
    4. Wykrywanie ataków typu brute force na różne usługi.
    5. Wykrywanie i przeciwdziałanie złośliwemu oprogramowaniu.
    6. Analiza logów w oparciu o wbudowane reguły bezpieczeństwa.
    7. Konfiguracja oprogramowania do przechowywania logów z kluczowych zasobów przez okres 24 miesięcy zgodnie z rozporządzeniem KRI §21 pkt. 4 „Informacje w dziennikach systemów przechowywane są od dnia ich zapisu, przez okres wskazany w przepisach odrębnych, a w przypadku braku przepisów odrębnych przez dwa lata.”
    8. Panel do wyszukiwania zdarzeń.

2. Wdrożenie systemu.
   1. Wykonawca będzie odpowiedzialny za instalację i konfigurację oraz optymalizację środowiska systemu w infrastrukturze Zamawiającego oraz opiekę serwisową i wsparcie techniczne przez okres 30 dni.
3. Wykonawca przeprowadzi instruktaż stanowiskowy dla Administratorów (zarządzających systemem), co najmniej w n/w zakresie:
   1. Przedstawienie architektury systemu.
   2. Omówienie procedur obsługi administracyjnej systemu;
   3. omówienie możliwości funkcjonalnych, zakresu dostępnych funkcji oraz ograniczeń systemu;
   4. przekazanie informacji na temat konfiguracji i zarządzania systemem;
   5. instruktaż stanowiskowy musi obejmować część teoretyczną i praktyczną.

21. Wdrożenie oprogramowania przeciwdziałającemu wyciekowi danych.

Usługi wdrożeniowe oprogramowania przeciwdziałającego wyciekowi danych (DLP), którego głównym celem jest zabezpieczenie przed utratą lub nieautoryzowanym dostępem do informacji poufnych. Oprogramowanie to ma zostać zainstalowane na serwerze działającym pod kontrolą systemu Windows Server co najmniej w wersji 2016 oraz powinno być obsługiwane za pomocą dwóch konsol: aplikacyjnej i webowej, w celu ułatwienia zarządzania systemem.

A. Wykonawca przeprowadzi analizę wymagań Zamawiającego, zaczynając od zebrania wymagań od różnych zespołów w organizacji, aby określić, jakie funkcje i moduły oprogramowania na stacjach roboczych, serwerach, urządzeniach sieciowych będą najbardziej przydatne.

B. Wykonawca przeprowadzi planowanie wdrożenia w oparciu o przeprowadzoną analizę, uwzględniając harmonogram, zasoby, zadania.

C. Wykonawca przygotuje środowisko wirtualne, upewniając się, że wszystkie wymagania stawiane przez oprogramowanie zostały spełnione, włączając w to odpowiednie zasoby, konfigurację systemu operacyjnego oraz konfigurację sieciową niezbędną do prawidłowego działania oprogramowania.

D. Wykonawca wykona konfigurację baz danych niezbędnych do wdrożenia oprogramowania, włączając to prawidłowe połączenie pomiędzy oprogramowaniem a bazą danych.

E. Wykonawca zainstaluje oprogramowanie przeciwdziałającego wyciekowi danych.

F. Wykonawca wykona integrację z istniejącymi systemami w środowisku Zamawiającego, w tym z kontrolerem domeny oraz przygotuje konta usługi oprogramowania, włączając w to konfigurację uprawnień dla konta usługi. Wykonawca przeprowadzi testy wykonanej integracji w celu upewnienia się, że informacje są poprawnie synchronizowane między oprogramowaniem a istniejącymi systemami w środowisku Zamawiającego, w tym z kontrolerem domeny oraz czy synchronizacja użytkowników, grup i innych obiektów z kontrolera domeny do oprogramowania działa w sposób prawidłowy. Wykonawca będzie monitorował i utrzymywał integrację między oprogramowaniem przez cały okres trwania wdrożenia.

G. Wykonawca uruchomieni i skonfiguruje konsolę zarządzającą, wprowadzi klucz dostępowy i usunie dane demonstracyjne.

H. Wykonawca przeprowadzi instruktaż w zakresie prawidłowej instalacji agentów niezbędnych do prawidłowego działania oprogramowania, uwzględniając utworzenie odpowiednich grup i polityk wdrożeniowych dla agentów. Po zakończonej instalacji agentów, Wykonawca przeprowadzi testy poprawności instalacji i komunikacji agentów z serwerem oprogramowania.

I. Wykonawca przeprowadzi testy instalacji w celu upewnienia się, że instalacja oprogramowania przebiegła bez problemów i wszystkie komponenty zostały poprawnie zainstalowane na serwerze oraz urządzeniach końcowych.

J. Wykonawca wykona konfigurację kategorii danych i danych wrażliwych oraz zdefiniuje wykrywanie kategorii:

- Numery kart kredytowych

- Numery IBAN
- Numery dowodów osobistych
- Polski numer paszportu
- Numer PESEL

K. Wykonawca skonfiguruje alerty związane z usługami oraz zabezpieczeniem DLP oraz przetestuje poprawność ich działania na danych testowych.

L. Wykonawca skonfiguruje zadania archiwizacji danych oraz usuwania starych wpisów z bazy danych.

M. Wykonawca przetestuje działanie polityk i wprowadzi ich aktualizację w przypadku wykrycia braku ich skutecznego działania.

N. Wykonawca wygeneruje z prawidłowo wdrożonego oprogramowania raport audytu bezpieczeństwa
i przeprowadzi analizę aktywności użytkowników oraz przepływu informacji w organizacji.

O. Wykonawca przeprowadzi testy monitorowania i raportowania, weryfikując czy raporty generowane przez oprogramowanie zawierają poprawne i aktualne informacje.

P. Wykonawca przeprowadzi testy wydajnościowe w celu upewnienia się, że infrastruktura oprogramowania działa płynnie i efektywnie, nawet przy dużej liczbie urządzeń i użytkowników.

Q. Wykonawca przeprowadzi testy przywracania awaryjnego, włączając w to procedury przywracania awaryjnego w celu upewnienia się, że w razie konieczności można szybko przywrócić działanie systemu oprogramowania sieciowych po awarii.

22. Utrzymanie systemów teleinformatycznych.

Usługi stałego wsparcia technicznego (II linia wsparcia IT)

Przedmiotem zamówienia jest świadczenie usług stałej opieki informatycznej dla Zamawiającego, obejmujących w ilości nie mniejszej niż 120 godzin oraz w okresie nie krótszym niż 12 miesięcy:

- pomoc zdalna w rozwiązywaniu problemów z serwerami i oprogramowaniem serwerowym;
- monitorowanie dostępności serwerów i usług;
- reagowanie na problemy związane z dostępnością serwerów;
- zarządzanie zmianami i wersjami oprogramowania serwerowego;
- instalacja i konfiguracja nowego oprogramowania i sprzętu;
- zarządzanie patchami i aktualizacjami oprogramowania;
- backup i odzyskiwanie danych;
- monitorowanie wydajności systemów i aplikacji;
- diagnozowanie i rozwiązywanie problemów z wydajnością;
- zarządzanie konfiguracją systemów i aplikacji;
- automatyzacja rutynowych zadań operacyjnych;
- analiza i interpretacja logów systemowych i aplikacji;
- reagowanie na alerty bezpieczeństwa generowane przez SIEM;
- analiza trendów i przewidywanie przyszłych problemów;
- wdrażanie i zarządzanie kontenerami i usługami mikrousług;
- konfiguracja i zarządzanie sieciami wirtualnymi;
- zarządzanie certyfikatami SSL/TLS;
- wdrażanie zasad bezpieczeństwa i konfiguracji firewalli;
- audyt konfiguracji i zabezpieczeń systemów;
- przeprowadzanie testów penetracyjnych i ocen ryzyka;
- zarządzanie użytkownikami i uprawnieniami;
- zarządzanie bazami danych (backup, tuning, aktualizacje);
- zarządzanie środowiskami deweloperskimi, testowymi i produkcyjnymi;
- wsparcie dla procesów CI/CD (Continuous Integration/Continuous Deployment);
- doradztwo w zakresie architektury systemów i aplikacji;

- optymalizacja kosztów usług chmurowych;
- zarządzanie kluczami szyfrowania i dostępem do danych wrażliwych;
- planowanie i testowanie ciągłości działania (DR/BCP);
- zarządzanie incydentami bezpieczeństwa i reagowanie na nie;
- konsultacje w zakresie najlepszych praktyk DevOps i bezpieczeństwa IT;
- analiza przyczynowa (Root Cause Analysis) dla incydentów IT;
- zarządzanie dokumentacją techniczną i operacyjną;
- wsparcie przy migracjach systemów i aplikacji;
- ocena zgodności z wymaganiami regulacyjnymi i standardami branżowymi;
- szkolenia użytkowników i personelu technicznego w zakresie obsługi systemów;
- monitorowanie zagrożeń w cyberprzestrzeni i aktualizacja zabezpieczeń;
- zarządzanie konfiguracją sieci i urządzeń sieciowych;
- ocena skuteczności zaimplementowanych środków bezpieczeństwa;
- wsparcie dla procesów skalowania infrastruktury IT;
- analiza potrzeb biznesowych i doradztwo technologiczne;
- optymalizacja procesów biznesowych za pomocą technologii IT;
- przeglądy architektury systemów pod kątem najlepszych praktyk i zaleceń;
- wsparcie w zakresie integracji systemów i aplikacji;
- zarządzanie środowiskami wirtualnymi i chmurowymi;
- ocena wykorzystania zasobów IT i rekomendacje dotyczące optymalizacji;
- zarządzanie zmianą w infrastrukturze IT i procesach operacyjnych.

Zadania będą realizowane selektywnie i niezwłocznie na każde wezwanie Zamawiającego w godzinach 8:00 – 16:00 oraz w przypadku problemów krytycznych, przez całą dobę.

23. Utrzymanie stałego wsparcia technicznego i organizacyjnego w zakresie utrzymania i doskonalenia wdrożonych standardów bezpieczeństwa .

1. Cel zamówienia.

Celem zamówienia jest wzmocnienie mechanizmów bezpieczeństwa oraz poprawa zgodności operacyjnej systemów teleinformatycznych Zamawiającego z wymogami stawianymi przez ROZPORZĄDZENIE 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, zwłaszcza w zakresie monitorowania i przeglądania oraz utrzymywania i doskonalenia systemu zarządzania bezpieczeństwem informacji zapewniającego poufność, dostępność i integralność informacji z uwzględnieniem takich atrybutów, jak autentyczność, rozliczalność, niezaprzeczalność i niezawodność, w oparciu o normy:

a. PN-ISO/IEC 27001 - w odniesieniu do formy systemu zarządzania bezpieczeństwem informacji;
b. PN-ISO/IEC 27002 - w odniesieniu do ustanawiania zabezpieczeń;
c. PN-ISO/IEC 27005 - w odniesieniu do zarządzania ryzykiem;
d. PN-ISO/IEC 24762 - w odniesieniu do odtwarzania techniki informatycznej po katastrofie w ramach zarządzania ciągłością działania.

2. Zakres zamówienia.

Usługa będzie obejmować stałe doradztwo i wsparcie w ilości godzin nie mniejszej niż 120 godzin oraz w okresie nie krótszym niż 12 miesięcy w celu optymalizacji procesów zarządzania bezpieczeństwem informacji przez zespół co najmniej 2 certyfikowanych audytorów, pełniących rolę Pełnomocnika ds. Systemu Zarządzania Bezpieczeństwem Informacji, posiadających łącznie co najmniej poniższe certyfikaty:

a. 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 2018 r. poz. 650 i 1338), w zakresie certyfikacji osób;

I-I.271.11.2024 Gorzyce, 15.07.2024 r.

b. 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.

Usługa obejmować będzie również:

a. zapewnienie aktualizacji regulacji wewnętrznych w zakresie zmieniającego się otoczenia;

b. kontrolę aktualności inwentaryzacji sprzętu i oprogramowania służącego do przetwarzania informacji, obejmującej ich rodzaj i konfigurację;

c. przeprowadzanie okresowych analiz ryzyka utraty integralności, dostępności lub poufności informacji oraz sugerowanie działań minimalizujących to ryzyko, stosownie do wyników przeprowadzonej analizy;

d. podejmowanie działań zapewniających, że osoby zaangażowane w proces przetwarzania informacji posiadają stosowne uprawnienia i uczestniczą w tym procesie w stopniu adekwatnym do realizowanych przez nie zadań oraz obowiązków mających na celu zapewnienie bezpieczeństwa informacji;

e. bezzwłoczną zmianę uprawnień w przypadku zmiany zadań osób, o których mowa w podpunkcie d;

f. zapewnienie szkolenia osób zaangażowanych w proces przetwarzania informacji, ze szczególnym uwzględnieniem zagadnień takich jak zagrożenia bezpieczeństwa informacji, skutki naruszenia zasad bezpieczeństwa informacji, w tym odpowiedzialność prawna, stosowanie środków zapewniających bezpieczeństwo informacji, w tym urządzenia i oprogramowanie minimalizujące ryzyko błędów ludzkich;

g. wsparcie w zakresie aktualizacji technicznych i organizacyjnych środków ochrony przetwarzanych informacji przed ich kradzieżą, nieuprawnionym dostępem, uszkodzeniami lub zakłóceniami poprzez monitorowanie dostępu do informacji, działania zmierzające do wykrycia nieautoryzowanych działań związanych z przetwarzaniem informacji, zapewnienie środków uniemożliwiających nieautoryzowany dostęp na poziomie systemów operacyjnych, usług sieciowych i aplikacji;

h. ustanowienie podstawowych zasad gwarantujących bezpieczną pracę przy przetwarzaniu mobilnym
i pracy na odległość;

i. wsparcie merytoryczne w zakresie zabezpieczenia informacji w sposób uniemożliwiający nieuprawnionemu jej ujawnienie, modyfikacje, usunięcie lub zniszczenie;

j. weryfikację zapisów w umowach serwisowych podpisanych ze stronami trzecimi, gwarantujących odpowiedni poziom bezpieczeństwa informacji;

k. ustalenie zasad postępowania z informacjami, zapewniających minimalizację wystąpienia ryzyka kradzieży informacji i środków przetwarzania informacji, w tym urządzeń mobilnych;

l. wsparcie merytoryczne w zakresie zapewnienia odpowiedniego poziomu bezpieczeństwa w systemach teleinformatycznych, w szczególności w obszarach: dbałości o aktualizację oprogramowania, minimalizowania ryzyka utraty informacji w wyniku awarii, ochrony przed błędami, utratą, nieuprawnioną modyfikacją, stosowania mechanizmów kryptograficznych w sposób adekwatny do zagrożeń lub wymogów przepisu prawa, zapewnienia bezpieczeństwa plików systemowych, redukcji ryzyk wynikających z wykorzystania opublikowanych podatności technicznych systemów teleinformatycznych, niezwłocznego podejmowania działań po dostrzeżeniu nieujawnionych podatności systemów teleinformatycznych na możliwość naruszenia bezpieczeństwa, kontroli zgodności systemów teleinformatycznych z odpowiednimi normami i politykami bezpieczeństwa;

m. w przypadku pojawienia się incydentów naruszenia bezpieczeństwa informacji, wsparcie w bezzwłocznym zgłaszaniu w określony i z góry ustalony sposób do właściwych organów, umożliwiającym szybkie podejmowanie działań korygujących.

I-I.271.11.2024 Gorzyce, 15.07.2024 r.

24. Wdrożenie i szkolenie z oprogramowania do zarządzania i aktualizacji systemów operacyjnych na stacjach roboczych, serwerach, urządzeniach sieciowych oraz monitorowania infrastruktury informatycznej.

Usługi wdrożeniowe oprogramowania do zarządzania i aktualizacji systemów operacyjnych na stacjach roboczych, serwerach, urządzeniach sieciowych oraz monitorowania infrastruktury informatycznej.

A. Wykonawca przeprowadzi analizę wymagań Zamawiającego, zaczynając od zebrania wymagań od różnych zespołów w organizacji, aby określić, jakie funkcje i moduły oprogramowania na stacjach roboczych, serwerach, urządzeniach sieciowych będą najbardziej przydatne.

B. Wykonawca przeprowadzi planowanie wdrożenia w oparciu o przeprowadzoną analizę, uwzględniając harmonogram, zasoby, zadania.

C. Wykonawca przygotuje środowisko wirtualne, upewniając się, że wszystkie wymagania stawiane przez oprogramowanie zostały spełnione, włączając w to odpowiednie zasoby, konfigurację systemu operacyjnego oraz konfigurację sieciową niezbędną do prawidłowego działania oprogramowania.

D. Wykonawca wykona konfigurację baz danych niezbędnych do wdrożenia oprogramowania, włączając to prawidłowe połączenie pomiędzy oprogramowaniem a bazą danych.

E. Wykonawca zainstaluje oprogramowanie do zarządzania i aktualizacji systemów operacyjnych i oprogramowania do zarządzania i aktualizacji systemów operacyjnych na stacjach roboczych, serwerach, urządzeniach sieciowych oraz monitorowania infrastruktury informatycznej, na wskazanym serwerze lokalnym lub w chmurze i skonfiguruje je zgodnie z wymaganiami i najlepszymi praktykami.

F. Wykonawca wykona integrację z istniejącymi systemami w środowisku Zamawiającego, w tym z kontrolerem domeny oraz przygotuje konta usługi oprogramowania, włączając w to konfigurację uprawnień dla konta usługi. Wykonawca przeprowadzi testy wykonanej integracji w celu upewnienia się, że informacje są poprawnie synchronizowane między oprogramowaniem a istniejącymi systemami w środowisku Zamawiającego, w tym z kontrolerem domeny oraz czy synchronizacja użytkowników, grup i innych obiektów z kontrolera domeny do oprogramowania działa w sposób prawidłowy. Wykonawca będzie monitorował i utrzymywał integrację między oprogramowaniem przez cały okres trwania wdrożenia.

G. Wykonawca przeprowadzi instruktaż w zakresie prawidłowej instalacji agentów niezbędnych do prawidłowego działania oprogramowania, uwzględniając utworzenie odpowiednich grup i polityk wdrożeniowych dla agentów. Po zakończonej instalacji agentów, Wykonawca przeprowadzi testy poprawności instalacji i komunikacji agentów z serwerem oprogramowania.

H. Wykonawca przeprowadzi testy instalacji w celu upewnienia się, że instalacja oprogramowania przebiegła bez problemów i wszystkie komponenty zostały poprawnie zainstalowane na serwerze.

I. Wykonawca przeprowadzi testy zarządzania urządzeniami, w tym możliwość dodawania, usuwania
i zarządzania urządzeniami w konsoli administracyjnej oprogramowania oraz poprawność wykonywania instalacji, aktualizacji i usuwania oprogramowania. Wykonawca przetestuje, że konfiguracje mogą być efektywnie stosowane na wybranych urządzeniach.

J. Wykonawca przeprowadzi testy zdalnego zarządzania poprzez zdalne sterowanie komputerem oraz zdalne wsparcie ekranowe. Wykonawca w ramach tego zadania zweryfikuje dodatkowo czy można efektywnie udzielać pomocy technicznej użytkownikom poprzez konsolę oprogramowania.

K. Wykonawca przeprowadzi testy monitorowania i raportowania, weryfikując czy raporty generowane przez oprogramowanie zawierają poprawne i aktualne informacje na temat stanu infrastruktury IT oraz czy możliwość monitorowania wydajności urządzeń i systemów za pomocą narzędzi dostępnych w oprogramowaniu działa prawidłowo, zgodnie z założeniami prawidłowego działania oprogramowania.

L. Wykonawca przeprowadzi testy zabezpieczeń, weryfikując czy zastosowane zabezpieczenia, takie jak zasady bezpieczeństwa i ochrona antywirusowa, są skutecznie wdrażane na urządzeniach.

I-I.271.11.2024 Gorzyce, 15.07.2024 r.

M. Wykonawca przeprowadzi testy wydajnościowe w celu upewnienia się, że infrastruktura oprogramowania działa płynnie i efektywnie, nawet przy dużej liczbie urządzeń i użytkowników.

N. Wykonawca przeprowadzi testy przywracania awaryjnego, włączając w to procedury przywracania awaryjnego w celu upewnienia się, że w razie konieczności można szybko przywrócić działanie systemu oprogramowania sieciowych po awarii

Szkolenie z obsługi oprogramowania do zarządzania i aktualizacji systemów operacyjnych na stacjach roboczych, serwerach, urządzeniach sieciowych oraz monitorowania infrastruktury informatycznej

Przedmiotem zamówienia jest przeprowadzenie szkolenia stacjonarnego lub online dla personelu IT, w celu przekazania kompletnej wiedzy w zakresie obsługi i wykorzystania funkcji oprogramowania zarządzania i aktualizacji systemów operacyjnych na stacjach roboczych, serwerach, urządzeniach sieciowych oraz monitorowania infrastruktury informatycznej w ich codziennej pracy.

Szkolenie obejmie co najmniej następujące obszary:

O. Wprowadzenie do oprogramowania do zarządzania i aktualizacji systemów operacyjnych i oprogramowania na stacjach roboczych, serwerach, urządzeniach sieciowych: Omówienie podstawowych koncepcji związanych z oprogramowaniem do zarządzania i aktualizacji systemów operacyjnych
i oprogramowania na stacjach roboczych, serwerach, urządzeniach sieciowych, takich jak zarządzanie urządzeniami, oprogramowaniem i konfiguracjami.

P. Interfejs użytkownika: Przewodnik po interfejsie użytkownika oprogramowania do zarządzania i aktualizacji systemów operacyjnych i oprogramowania na stacjach roboczych, serwerach, urządzeniach sieciowych, pokazujący główne funkcje i narzędzia dostępne dla administratorów.

Q. Zarządzanie urządzeniami: Szkolenie w zakresie dodawania, konfigurowania i monitorowania urządzeń oprogramowania do zarządzania i aktualizacji systemów operacyjnych i oprogramowania na stacjach roboczych, serwerach, urządzeniach sieciowych, w tym zarządzanie grupami i politykami.

R. Zarządzanie oprogramowaniem: Instrukcje dotyczące instalowania, aktualizowania i monitorowania oprogramowania na urządzeniach za pomocą oprogramowania do zarządzania i aktualizacji systemów operacyjnych i oprogramowania na stacjach roboczych, serwerach, urządzeniach sieciowych.

S. Automatyzacja procesów: Szkolenie związane z automatyzacją rutynowych zadań administracyjnych za pomocą skryptów i zadań zaplanowanych dla oprogramowania do zarządzania i aktualizacji systemów operacyjnych i oprogramowania na stacjach roboczych, serwerach, urządzeniach sieciowych.

T. Bezpieczeństwo: Omówienie funkcji związanych z zabezpieczeniami oprogramowania do zarządzania i aktualizacji systemów operacyjnych i oprogramowania na stacjach roboczych, serwerach, urządzeniach sieciowych, takich jak zarządzanie aktualizacjami, ochrona przed złośliwym oprogramowaniem i polityki bezpieczeństwa.

U. Wsparcie użytkowników końcowych: Instrukcje dotyczące udzielania pomocy technicznej użytkownikom końcowym oraz rozwiązywania problemów związanych z urządzeniami i oprogramowaniem.

V. Raportowanie i analiza: Szkolenie z generowania raportów i analizy danych dla oprogramowania do zarządzania i aktualizacji systemów operacyjnych i oprogramowania na stacjach roboczych, serwerach, urządzeniach sieciowych w celu monitorowania wydajności i zgodności z wymaganiami.

W. Scenariusze praktyczne: Przeprowadzenie praktycznych ćwiczeń i scenariuszy, aby umożliwić uczestnikom praktyczne zastosowanie wiedzy zdobytej podczas szkolenia.

X. Ewaluacja: Przeprowadzenie ewaluacji, aby ocenić skuteczność szkolenia i zidentyfikować obszary do dalszego doskonalenia.

Czas trwania szkolenia przewidziano na co najmniej 4 dni roboczy z uwzględnieniem przerw 3 przerw po 15 minut.

Po szkoleniu Wykonawca udostępni **co** najmniej 4 godziny robocze na dodatkowe pytania i odpowiedzi uczestników przez okres 30 dni.

I-I.271.11.2024 Gorzyce, 15.07.2024 r.

25. Testy penetracyjne.

Wykonawca posiada potencjał techniczny i osobowy niezbędny do wykonania zamówienia.
Potencjał techniczny przedstawia się poprzez posiadanie narzędzi takich jak automatyczny skaner podatności posiadający funkcje pozwalające na:

- wykonanie skanowań z wykorzystaniem wbudowanych szablonów;
- skanowanie sieciowe (wykrywanie otwartych portów i rozpoznanie uruchomionych na nich usług, wskazywanie listy podatności na wykryte usługi);
- weryfikacje domyślnych haseł według zadanego słownika;
- skanowanie systemów operacyjnych z uwierzytelnieniem (sprawdzenie wersji systemu, zainstalowanych na nim aplikacji, brakujących aktualizacji, wskazywanie listy podatności na wykryte systemy
i aplikacje) oraz weryfikację uprawnień zadanego użytkownika;
- ustawienia harmonogramu skanowań;
- możliwość porównania wyników poszczególnych skanowań;
- możliwość konfigurowania zawartości raportu ze skanowania oraz dobieranie różnych formatów wyjściowych raportów (w tym HTML, CVS i XML);
- możliwość wyświetlania wyników na bieżąco oraz możliwość grupowania podobnej klasy podatności
i możliwość sortowania po IP i podatnościach.

Aplikacje do testów stron i aplikacji internetowych posiadającej funkcje pozwalające na:

- przechwytywanie wszystkich zapytań i odpowiedzi pomiędzy przeglądarką a aplikacją docelową, nawet gdy używany jest HTTPS;
- przeglądanie, edytowanie oraz upuszczanie pojedynczych wiadomości, w celu manipulacji komponentami aplikacji po stronie serwera lub klienta;
- dodawanie adnotacji do poszczególnych elementów w celu ich oznaczenia do późniejszego sprawdzenia;
- wykonywanie różnych automatycznych modyfikacji odpowiedzi w calu ułatwienia testowania;
- tworzenie reguł dopasowywania i zastępowania do automatycznego stosowania własnych modyfikacji do żądań i odpowiedzi przechodzących przez serwer Proxy;
- precyzyjna konfiguracja reguł przechwytywania wiadomości;
- możliwość wyeliminowania ostrzeżeń bezpieczeństwa przeglądarki, mogących się pojawiać podczas przechwytywania połączeń HTTPS;
- pokazanie całej zawartości odkrytej podczas testowania umieszczana na mapie skanowanej witryny. Treść prezentowana w widoku drzewa, odpowiadającego strukturze stron URL;
- żądania i odpowiedzi dostępne w edytorze http;
- narzędzie do ręcznej edycji i ponownego wstawiania żądań;
- narzędzie do analizy statystycznej tokenów sesji;
- możliwość zapisu pracy na poszczególnych etapach w czasie rzeczywistym oraz powrót do zapisanego miejsca;
- biblioteka konfiguracji do szybkiego uruchomienia ukierunkowanego skanowania z różnymi ustawieniami;
- możliwość ręcznego umieszczania punktów wstawiania w dowolnych miejscach żądania, w celu poinformowania skanera o niestandardowych formatach danych i wejściach;
- skanowanie na żywo podczas przeglądania, zapewniające pełną kontrolę nad działaniami wykonywanymi dla żądań;
- możliwość analizy docelowej aplikacji internetowych.
- narzędzie do automatycznego przechwytywania szczegółowych wyników o niestandardowych atakach na aplikacje.

Potencjał osobowy przedstawia się poprzez posiadanie przez osoby testujące łącznie takie certyfikaty jak: OSCP (offensice security), CEH (EC-Council), Burp Suite Certified Practitioner (PortSwinger), eWPTX (eLearnSecurity),

eCPPT (eLearnSecurity). Skanowania nie mogą być realizowane tylko z wykorzystaniem narzędzi automatycznych, konieczna jest manualna weryfikacja podatności znalezionych w testach automatycznych. Przeprowadzenie testów nie może wymagać od Zamawiającego zakupu żadnych dodatkowych licencji lub wyposażenia.
W ramach przeprowadzonych testów penetracyjnych infrastruktury, Wykonawca wykona:

1. Rekonesans.
   a. Zgromadzenie wszystkich dostępnych publicznie informacji nt. osób reprezentujących instytucję
      w celu stworzenia potencjalnej bazy loginów i haseł.
   b. Zgromadzenie informacji nt. zasobów instytucji dostępnych publicznie (strona internetowa, serwer www, serwer ftp, inne usługi).
   c. zgromadzenie informacji nt. potencjalnie niejawnych zasobów dostępnych dla wyszukiwarek internetowych.
   d. Sprawdzenie występowania w wyciekach znalezionych loginów.
2. Enumeracja zasobów.
   a. Analiza zasobów zidentyfikowanych w pkt. 1 w celu określenia precyzyjnej listy aplikacji (wraz
      z określeniem ich wersji) działających w ramach usług.
   b. Skanowanie publicznej infrastruktury.
   c. Skanowanie wewnętrznej infrastruktury z wykorzystaniem automatycznego skanera podatności.
   d. Sprawdzenie udostępnionych w sieci wewnętrzej plików i folderów w szczególności pod kątem występowania danych wrażliwych.
   e. Analiza dostępnych wewnątrz sieci, usług, protokołów i urządzeń.
3. Eksploitacja.
   a. Próba zalogowania do zidentyfikowanych zasobów, m.in. z użyciem list stworzonych w pkt. 1, także logowanie typu brute-force oraz domyślnych haseł.
   b. Wykorzystanie podatności ujawnionych na etapie enumeracji (cve dla znanych wersji aplikacji) – po uzgodnieniu z Zamawiającym.
   c. Analiza konfiguracji dostępnych środowisk w celu wykorzystania jej błędów (analiza hardeningu, architektury sieci, błędy w konfiguracji serwera www i architektury aplikacji internetowych oraz innych usług).
4. Eskalacja uprawnień.
   a. Wykorzystanie zasobów skompromitowanych w pkt. 3 w celu ewentualnego podniesienia uprawnień.
   b. Rozpoznanie zasobów wewnętrznych, przechodzenie na inne środowiska dostępne ze skompromitowanych w pkt.3 zasobów (lateral movement).
5. Raport z testu penetracyjnego.

Wykonawca dostarczy raport zawierający:

1. Podsumowanie dla kierownictwa.
2. Opis zakresu wykonanych prac.
3. Wyłączenia z testów jeżeli były.
4. Listę danych zebranych w trakcie rekonesansu (w tym listę zidentyfikowanych adresów IP w sieci wewnętrznej).
5. Listę znalezionych podatności wraz z określoną dla niej waga zgodnie z ze standardem Common Vulnerability Scoring System Version 4.0 oraz modelem STRIDE.
6. Szczegółowy opis znalezionych podatności.
7. Zalecenia naprawy nieprawidłowości bądź mitygacji zagrożeń z nich wynikających.

26. Szkolenia powiązane z testami socjotechnicznym.

1. Przygotowanie kampanii socjotechnicznej;

a. wybór i zakup przez Wykonawcę domeny (łudząco podobnej do domeny Zamawiającego), która zostanie wykorzystana do kampanii socjotechnicznej;
b. opracowanie bazy mailingowej pracowników objętych kampanią socjotechniczną oraz spreparowanego dokumentu zbliżonego wyglądem do dokumentów Zamawiającego, zawierającego dodatkowy niezłośliwy kod pozwalający na mierzenie efektów kampanii;
c. wyznaczenie osób wtajemniczonych w fakt przeprowadzania testów (np. najwyższe kierownictwo, dział informatyczny lub wyłącznie szef tego działu, inspektor ochrony danych lub inna osoba odpowiedzialna za bezpieczeństwo w organizacji);
d. wsparcie w zakresie dodania domeny wybranej do przeprowadzenia kampanii socjotechnicznej do tzw. białej/zaufanej listy w celu pominięcia filtrów antyspamowych (celem testu jest dostarczenie spreparowanej wiadomości na wszystkie skrzynki pracowników
i weryfikacja ich podatności na prawdziwe kampanie cyberprzestępców).

2. Przygotowanie spreparowanych zasobów służących wyłudzaniu informacji:
3. serwer strony www z bazą danych powiązany z domeną, która została zakupiona w celu przeprowadzenia kampanii socjotechnicznej;
4. wykonanie kopii strony internetowej Zamawiającego i umieszczenie jej pod spreparowanym adresem;
5. wygenerowanie niezbędnych certyfikatów SSL;
6. przygotowanie spreparowanego aktywnego dokumentu PDF, wyposażonego w autorski, niezłośliwy skrypt, którego celem jest zebranie informacji o użytkownikach, którzy dokonali otwarcia pliku PDF i uruchomienia niezłośliwego skryptu (w prawdziwej kampanii byłoby to złośliwe oprogramowanie);
7. utworzenie nowej podstrony, na której umieszczony zostanie spreparowany plik PDF;
8. przygotowanie konta mailowego, którego celem jest podszycie się pod jedną z osób wtajemniczonych w prowadzone testy phishingowe;
9. przygotowanie treści wiadomości e-mail i wyposażenie jej w mechanizmy pozwalające na przeprowadzenie tzw. detekcji umiejscowienia (uzyskanie adresu IP potencjalnej „ofiary").
10. Przeprowadzenie kampanii socjotechnicznej (wysłanie przygotowanej uprzednio wiadomości e-mail do pracowników wskazanych w bazie mailingowej).
11. Wykonanie raportu z testu socjotechnicznego w języku polskim.
12. Przeprowadzenie szkolenia dla pracowników z zakresu cyberbezpieczeństwa, ukierunkowanego na omówienie wyników kampanii socjotechnicznej oraz co najmniej:
13. wprowadzenie do cyberbezpieczeństwa:
    a. czym jest cyberbezpieczeństwo;
    b. dlaczego cyberbezpieczeństwo jest ważne;
    c. kluczowe zagadnienia związane z cyberbezpieczeństwem;
    d. przegląd statystyk i trendów w cyberbezpieczeństwie.
14. typy zagrożeń w cyberprzestrzeni:
    a. malware (wirusy, trojany, robaki itp.);
    b. ataki typu phishing i spear phishing;
    c. ataki DDoS;
    d. ataki ransomware;
    e. zagrożenia związane z sieciami społecznościowymi.
15. zasady bezpieczeństwa i praktyki:
    a. zarządzanie hasłami i uwierzytelnianie wieloskładnikowe;
    b. zasady bezpieczeństwa e-mail;
    c. bezpieczeństwo w sieciach bezprzewodowych;
    d. bezpieczne przeglądanie internetu;
    e. backup i odzyskiwanie danych.
16. reagowanie na incydenty i planowanie awaryjne:

a. jak zidentyfikować i zgłosić incydent związany z cyberbezpieczeństwem;
b. zasady reagowania na incydenty;
c. planowanie awaryjne i kontynuacja działalności;
d. Przegląd realnych przypadków naruszeń bezpieczeństwa i lekcje z nich wyniesione.

17. Czas trwania szkolenia przewidziano na co najmniej dwie grupy po 4 godziny robocze z uwzględnieniem przerw 15 minut w każdym szkoleniu. Po szkoleniu Wykonawca udostępni co najmniej 30 minut na pytania i odpowiedzi uczestników.

27. Szkolenie z cyberbezpieczeństwa dla kadry administracyjnej.

Przedmiotem zamówienia jest przeprowadzenie szkoleń z zakresu cyberbezpieczeństwa dla pracowników administracyjnych.
Szkolenie stacjonarne lub online z zakresu cyberbezpieczeństwa skierowane do pracowników administracyjnych, obejmujące co najmniej następujące obszary:

a. wprowadzenie do cyberbezpieczeństwa:
   - czym jest cyberbezpieczeństwo;
   - dlaczego cyberbezpieczeństwo jest ważne;
   - kluczowe zagadnienia związane z cyberbezpieczeństwem;
   - przegląd statystyk i trendów w cyberbezpieczeństwie.

b. typy zagrożeń w cyberprzestrzeni:
   - malware (wirusy, trojany, robaki itp.);
   - ataki typu phishing i spear phishing;
   - ataki DDoS;
   - ataki ransomware;
   - zagrożenia związane z sieciami społecznościowymi.

c. zasady bezpieczeństwa i praktyki:
   - zarządzanie hasłami i uwierzytelnianie wieloskładnikowe;
   - zasady bezpieczeństwa e-mail;
   - bezpieczeństwo w sieciach bezprzewodowych;
   - bezpieczne przeglądanie internetu;
   - backup i odzyskiwanie danych.

d. reagowanie na incydenty i planowanie awaryjne:
   - jak zidentyfikować i zgłosić incydent związany z cyberbezpieczeństwem;
   - zasady reagowania na incydenty;
   - planowanie awaryjne i kontynuacja działalności;
   - Przegląd realnych przypadków naruszeń bezpieczeństwa i lekcje z nich wyniesione.

Czas trwania szkolenia przewidziano na co najmniej dwie grupy po 4 godziny robocze z uwzględnieniem przerw 15 minut w każdym szkoleniu. Po szkoleniu Wykonawca udostępni co najmniej 30 minut na pytania i odpowiedzi uczestników.

28. Szkolenie z cyberbezpieczeństwa dla kadry informatycznej.

Przedmiotem zamówienia jest przeprowadzenie szkolenia z zakresu cyberbezpieczeństwa.
Indywidualne warsztaty online z zakresu cyberbezpieczeństwa skierowane do administratorów sieci teleinformatycznej, obejmujące co najmniej następujące obszary:

1. Wprowadzenie do cyberbezpieczeństwa:
   - Czym jest cyberbezpieczeństwo?
   - Dlaczego cyberbezpieczeństwo jest ważne?
   - Kluczowe zagadnienia związane z cyberbezpieczeństwem.
   - Przegląd statystyk i trendów w cyberbezpieczeństwie.
2. Typy zagrożeń w cyberprzestrzeni:
   - Malware (wirusy, trojany, robaki itp.)
   - Ataki typu phishing i spear phishing

- Ataki DDoS
- Ataki ransomware
- Zagrożenia związane z sieciami społecznościowymi.

3. Zasady bezpieczeństwa i praktyki:
   - Zarządzanie hasłami i uwierzytelnianie wieloskładnikowe
   - Zasady bezpieczeństwa e-mail
   - Bezpieczeństwo w sieciach bezprzewodowych
   - Bezpieczne przeglądanie internetu
   - Backup i odzyskiwanie danych
4. Bezpieczeństwo systemów i sieci
   - Zasady bezpieczeństwa systemów operacyjnych
   - Bezpieczeństwo sieci i firewall
   - Wprowadzenie do VPN
   - Bezpieczeństwo urządzeń IoT
   - Bezpieczeństwo w chmurze
5. Reagowanie na incydenty i planowanie awaryjne
   - Jak zidentyfikować i zgłosić incydent związany z cyberbezpieczeństwem
   - Zasady reagowania na incydenty
   - Planowanie awaryjne i kontynuacja działalności
   - Przegląd realnych przypadków naruszeń bezpieczeństwa i lekcje z nich wyniesione
6. Aktualne trendy i przyszłość cyberbezpieczeństwa
   - Sztuczna inteligencja i machine learning w cyberbezpieczeństwie
   - Kryptografia i blockchain
   - Bezpieczeństwo danych w erze Big Data
   - Przyszłość cyberbezpieczeństwa: wyzwania i możliwości

Czas trwania szkolenia przewidziano na 8 godzin roboczych w podziale na 2 dni szkoleniowe po 4 godziny roboczych z uwzględnieniem 4 przerw po 15 minut. Po każdym dniu szkolenia będzie 30 minut na pytania i odpowiedzi uczestników.

29. Szkolenie specjalistyczne dla kadry zarządzającej.

Cel szkolenia:

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

Struktura programu szkoleniowego:

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

W ramach przeprowadzonego szkolenia wykonawca przekaże:

1. Podstawowe informacje o obecnej sytuacji rynkowej powiązanej z tematyką cyberbezpieczeństwa:

- Podstawy i definicje: zapewnienie uczestnikom solidnych podstaw w dziedzinie cyberbezpieczeństwa poprzez omówienie kluczowych pojęć i zasad. Ponadto, zostanie przedstawiona rola menedżera w formowaniu bezpiecznego środowiska cyfrowego, co pozwoli zrozumieć jak ważne jest aktywne zaangażowanie kierownictwa w procesy zapewnienia bezpieczeństwa informacji. W ten sposób uczestnicy będą mieć pełniejsze zrozumienie zarówno teoretycznych, jak i praktycznych aspektów cyberbezpieczeństwa oraz będą lepiej przygotowani do podejmowania decyzji w tym obszarze.

I-I.271.11.2024 Gorzyce, 15.07.2024 r.

- Statystyki i trendy: skoncentrowanie się na przekazaniu uczestnikom szczegółowej analizy globalnych i lokalnych danych dotyczących cyberataków. Poprzez omówienie ewolucji tych ataków oraz ich metodologii, uczestnicy zyskają wgląd w aktualne trendy i sposoby działania cyberprzestępców. Ponadto, zostaną przedstawione skutki, jakie cyberatak może mieć dla biznesu, co pozwoli uczestnikom lepiej zrozumieć znaczenie inwestycji w bezpieczeństwo informacji oraz skuteczne zarządzanie ryzykiem cybernetycznym dla organizacji. Dzięki temu będą mogli podejmować bardziej świadome decyzje w zakresie ochrony swoich danych i infrastruktury cyfrowej.

2. Omówienie światowych standardów i norm w zakresie cyberbezpieczeństwa i bezpieczeństwa informacji:

- Normy ISO/IEC: Szczegółowe omówienie serii norm: ISO/IEC 27000: (zarysowuje leksykon oraz globalne zasady nadrzędne systemu zarządzania bezpieczeństwem informacji, kreśląc fundament pod szersze zrozumienie oraz efektywniejsze stosowanie pozostałych norm z rodziny 27000), ISO/IEC 27001 (stanowi kanon dotyczący wymagań dla systemów zarządzania bezpieczeństwem informacji, umożliwiając organizacjom zabezpieczenie informacji pod kątem ich poufności, integralności oraz dostępności przez implementację adekwatnych procedur zarządczych), ISO/IEC 27002 (oferuje referencyjny zbiór praktyk dla organizacji dążących do identyfikacji, wdrażania, utrzymania oraz doskonalenia swoich mechanizmów ochrony informacji w kontekście SZBI), ISO/IEC 27004 (dostarcza metodykę do monitorowania, przeglądu, oceny oraz doskonalenia efektywności systemu zarządzania bezpieczeństwem informacji, akcentując znaczenie mierzalnych wskaźników), ISO/IEC 27005 (zawiera wytyczne dotyczące zarządzania ryzykiem w kontekście bezpieczeństwa informacji, nakreślając proces identyfikacji, oceny oraz zarządzania ryzykiem informacyjnym), ISO/IEC 27006 (określa wymogi dla organizacji świadczących usługi certyfikacji systemów zarządzania bezpieczeństwem informacji, wyznaczając ramy dla procesu audytu i certyfikacji), ISO/IEC 27013 (podaje wytyczne integrujące system zarządzania bezpieczeństwem informacji z systemem zarządzania usługami IT, promując koherentną i efektywną infrastrukturę zarządzania), ISO/IEC 27017 (koncentruje się na bezpieczeństwie informacji w chmurze, proponując kontrole oraz wytyczne dla dostawców i użytkowników usług przetwarzania w chmurze), ISO/IEC 27018 (ustanawia kodeks praktyk dla ochrony informacji osobowych w chmurze, zgodnie z wymaganiami prywatności i ochrony danych), ISO/IEC 22301 (specyfikuje wymogi dla systemów zarządzania ciągłością działania, umożliwiając organizacjom przygotowanie na incydenty zakłócające normalne funkcjonowanie), ISO/IEC 24762 (zawiera wytyczne dla usług odzyskiwania po awariach w centrach danych i innych środowiskach IT, podkreślając kluczowe elementy potrzebne do przywrócenia operacji IT po katastrofie, ISO/IEC 27036 (skupia się na zarządzaniu bezpieczeństwem informacji w relacjach między organizacjami, oferując wytyczne dotyczące bezpieczeństwa w outsourcingu i partnerstwach biznesowych), ISO/IEC 31000 (dostarcza wytyczne dotyczące zarządzania ryzykiem ogólnym, promując model zarządzania ryzykiem, który można dostosować do różnych typów organizacji i kontekstów), 13501-2 (norma ta przeprowadza proces kategoryzacji reakcji na ogień wyrobów używanych w budownictwie oraz elementów konstrukcyjnych budowli, określając ich parametry odporności na pożary i zachowanie w ekstremalnych warunkach termicznych), norma 1627 (stanowi kryteria odporne na nieautoryzowany dostęp przez systemy zamykające, jak okna, drzwi oraz osłony, hierarchizując je zgodnie z ich zdolnością do stawiania oporu przy próbach sforsowania), norma 12209-04 (wytycza wymagania techniczne oraz procedury badawcze dla mechanizmów blokujących w obszarze budowlanym, takich jak zamki mechaniczne wraz z ich komponentami, oceniając ich funkcjonalność oraz niezawodność.), norma 50131-1 (określa specyfikacje dla systemów alarmowych przeznaczonych do sygnalizacji prób włamania czy napadu, wyznaczając standardy dotyczące ich skuteczności oraz metodyki testowania).
- Omówienie znaczenia powyższych norm i ich w zapewnianiu wysokiego poziomu bezpieczeństwa informacji oraz praktycznego zastosowania w organizacjach.
- Inne standardy: Przedstawienie i dyskusja na temat innych standardów:

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

I-I.271.11.2024 Gorzyce, 15.07.2024 r.

- Rola powyższych zagranicznych standardów w kształtowaniu efektywnych polityk bezpieczeństwa w organizacjach.

3. Omówienie zaawansowanych strategii ochrony organizacji:

- Zarządzanie ryzykiem: Metody identyfikacji, oceny, mitygacji i monitorowania ryzyka cybernetycznego. Wykorzystanie narzędzi i technologii do analizy ryzyka.
- Wprowadzenie do zarządzania incydentami, zdefiniowanie incydentów i wektorów ataku: atak przeprowadzony
z nośnika wymiennego lub urządzenia peryferyjnego, atak wykorzystujący metody brute-force w celu złamania, degradacji lub zniszczenia systemów, sieci lub usług, ataki wykonane z poziomu witryny internetowej lub aplikacji internetowej, atak przeprowadzony za pośrednictwem wiadomości e-mail lub załącznika, naruszenia zasad dopuszczalnego użytkowania organizacji przez autoryzowanego użytkownika, z wyłączeniem powyższych kategorii, utrata lub kradzież urządzenia komputerowego lub nośnika używanego przez organizację, na przykład laptopa lub urządzenia typu smartfon.
- Szczegółowy opis i kroki zarządzania incydentami:
    - wykrywanie: inicjacja procesu inicjującego, mającego na celu detekcję niestandardowych aktywności lub zdarzeń infrastrukturalnych, które mogą sygnalizować potencjalne zagrożenia w obszarze cybernetycznym;
    - rejestrowanie: operacja dokumentacyjna, polegająca na chronologicznym zapisie zaobserwowanych dysfunkcji w dedykowanych bazach danych, by zapewnić dokumentację dowodową dla późniejszych faz postępowania;
    - analizowanie: metodyczne badanie zgromadzonych artefaktów zdarzeń w celu zrozumienia ich genezy, dynamiki oraz wpływu na ekosystem informacyjny;
    - klasyfikowanie: systematyzacja incydentów według ustalonego kodu klasyfikacyjnego, uwzględniająca ich naturę, zasięg oraz potencjalne konsekwencje dla organizacji.
    - priorytetyzowanie: alokacja zasobów reakcyjnych na bazie oceny krytyczności, która koresponduje
z możliwymi konsekwencjami incydentu dla misji instytucji;
    - podejmowanie działań naprawczych: inicjowanie interwencji korygujących mających na celu restytucję funkcji systemowych i prewencję przed podobnymi naruszeniami w przyszłości;
    - ograniczanie skutków incydentu: implementacja taktyk zaradczych, które mają za zadanie minimalizację negatywnych rezultatów incydentu oraz odbudowę stanu równowagi operacyjnej.
- Priorytetyzacja incydentów na 3 kategorie: krytyczny, wysoki, średni na podstawie poniższych opisów:
    - Priorytet krytyczny - Incydent wymaga niezwłocznego działania oraz zgłoszenia do właściwego CSIRT. Procesy wewnętrzne są sparaliżowane lub zakłócone w znaczącym stopniu. Istnieje wysokie ryzyko wycieku danych (np. danych osobowych) oraz utraty poufności, integralności i/lub dostępności informacji.
    - Priorytet wysoki - Incydent wymaga szybkiego działania oraz zgłoszenia do właściwego CSIRT w ciągu 24 godzin. Procesy wewnętrzne są częściowo zakłócone lub sparaliżowane. Istnieje niskie ryzyko wycieku danych (np. danych osobowych) oraz utraty poufności, integralności i/lub dostępności informacji.
    - Priorytet średni - Incydent prawdopodobnie nie wymaga niezwłocznego działania oraz zgłoszenia do właściwego CSIRT ze względu na brak symptomów działania z zewnątrz. Procesy wewnętrzne nie są sparaliżowane lub zakłócone w żadnym stopniu. Ryzyko wycieku danych (np. danych osobowych) oraz utraty poufności, integralności i/lub dostępności informacji nie występuje.
- Budowanie zespołów ds. bezpieczeństwa: Definicja ról, odpowiedzialności, umiejętności oraz ścieżek rozwoju dla członków zespołu bezpieczeństwa.
- Lista omówionych kompetencji w szkoleniu:
    - Szef działu bezpieczeństwa (kierownik, dyrektor);
    - Pełnomocnik ds. Bezpieczeństwa Informacji;

I-I.271.11.2024 Gorzyce, 15.07.2024 r.

- Specjalista ds. Zarządzania Ryzykiem;
- Specjalista ds. Zgodności;
- Specjalista ds. Bezpieczeństwa Fizycznego;
- Architekt Systemów Bezpieczeństwa;
- Koordynator Programu Bezpieczeństwa;
- Analityk Bezpieczeństwa (II linia wsparcia);
- Inżynier ds. Bezpieczeństwa (II linia wsparcia);
- Administrator Systemów Bezpieczeństwa (II linia wsparcia);
- Specjalista ds. Odpowiedzi na Incydenty (III linia wsparcia);
- Specjalista ds. Testów Penetracyjnych (III linia wsparcia);
- Specjalista ds. Testów Socjotechnicznych (III linia wsparcia).

4. Regulacje prawne i compliance:

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

5. Zarządzanie bezpieczeństwem w praktyce:

- Zrozumienie znaczenia typów licencji względem konieczności ich testowania:

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

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

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

30. Szkolenie z oprogramowania przeciwdziałającemu wyciekowi danych.

Szkolenie z obsługi oprogramowania przeciwdziałającego wyciekowi danych

Przedmiotem zamówienia jest przeprowadzenie szkolenia stacjonarnego lub online dla personelu IT, w celu przekazania kompletnej wiedzy w zakresie obsługi i wykorzystania funkcji oprogramowania przeciwdziałającego wyciekowi danych, w ich codziennej pracy.

Szkolenie obejmie co najmniej następujące obszary:

- Podstawowe informacje
- Licencjonowanie
- Wspierane systemy operacyjne
- Wdrożenie oprogramowania przeciwdziałającego wyciekowi danych
- Omówienie instalatora oprogramowania przeciwdziałającego wyciekowi danych
- Wdrożenie serwera oprogramowania przeciwdziałającego wyciekowi danych
- Wdrożenie agentów oprogramowania przeciwdziałającego wyciekowi danych
- Wdrożenie klientów oprogramowania przeciwdziałającego wyciekowi danych
- Uruchomienie modułu analitycznego
- Analiza wycieków danych
- Filtrowanie i raporty z analizy
- Uruchomienie modułu przeciwdziałającego wyciekowi danych
- Uruchomienie szyfrowania BitLockerem
- Konfiguracja dostępu do urządzeń i portów
- Interfejs webowy oprogramowania przeciwdziałającego wyciekowi danych
- Minimalne wymagania systemowe dla omawianego oprogramowania
- Instalacja oraz konfiguracja modułu webowego oprogramowania przeciwdziałającego wyciekowi danych
- Analiza zachowań
- Zarządzenie kategoriami produktywności
- Kontrola WWW i aplikacji
- Alerty, raporty i konserwacja

- Zaawansowane DLP dla oprogramowania przeciwdziałającego wyciekowi danych
- Reguły DLP – tryby polityk
- Reguły ogólne
- Reguły aplikacji
- Po co nam kategorie danych?
- Inteligentne wyszukiwanie danych osobowych
- Czym są tagi i do czego służą?
- Reguły tagowania dla aplikacji, stron oraz lokalizacji

31. Szkolenie AD / wirtualizacja / kopie zapasowe.

1. Szkolenie z zakresu Active Directory (AD):
Inicjatywa szkoleniowa dedykowana Active Directory ma za zadanie zapewnić uczestnikom wszechstronne przygotowanie do efektywnego zarządzania oraz ochrony infrastruktury Active Directory, stanowiąc fundament dla bezpiecznego i zrównoważonego zarządzania tożsamościami i dostępami w sieciowych ekosystemach organizacyjnych. Program szkoleniowy został skonstruowany tak, aby objąć spektrum zagadnień, począwszy od elementarnych, aż po zaawansowane moduły:
- Ekspozycja na Architekturę Active Directory: Wstępna faza szkolenia skupia się na dogłębnym zarysie roli i kardynalnego znaczenia infrastruktury Active Directory w procesach zarządzania identyfikowalnością użytkowników oraz moderacji dostępu. Uczestnicy zostaną wprowadzeni w kompleksową architekturę AD, eksplorując jej kluczowe usługi i funkcjonalności, w tym mechanizmy uwierzytelniania, autoryzacji oraz efektywne zarządzanie zasobami.
- Podstawy Konfiguracji i Administracji Obiektami w AD: Moduł ten kładzie nacisk na praktyczne aspekty tworzenia, konfiguracji i zarządzania obiektami takimi jak użytkownicy, grupy i komputery, działającymi w obrębie środowiska AD. Uczestnicy zdobędą umiejętności w zakresie procedur dodawania, usuwania i modyfikacji obiektów, korzystając z dedykowanych narzędzi administracyjnych.
- Wprowadzenie do Mechanizmów Polityk Grupowych: Szczegółowe omówienie i analiza roli polityk grup (Group Policy) w kontekście zarządzania konfiguracją i bezpieczeństwem infrastruktury AD. Szkolenie obejmuje metodyki tworzenia, aplikacji i administrowania politykami grupowymi, ukazując ich wpływ na regulacje i konfiguracje zarówno klientów, jak i serwerów w domenie.
- Implementacja Zasad Bezpieczeństwa w AD: Dyskusja na temat strategii i metodologii wzmocnienia zabezpieczeń infrastruktury AD, obejmująca zarządzanie uprawnieniami, monitorowanie aktywności w logach oraz konfigurację polityk bezpieczeństwa. Szkolenie podkreśla praktyczne podejście do identyfikacji, reagowania oraz efektywnego rozwiązywania incydentów bezpieczeństwa.
- Strategie Ochrony AD Przed Atakami: Analiza potencjalnych zagrożeń dla infrastruktury AD oraz zapewnienie szkolenia z procedur szybkiego reagowania i odtwarzania funkcjonalności systemu w przypadku wystąpienia ataków lub innych awarii. Ten segment szkolenia jest poświęcony rozwijaniu kompetencji w zakresie przeciwdziałania zagrożeniom, przywracania systemu do stanu operacyjnego oraz zapewnienia ciągłości działania krytycznych usług.
2. Szkolenie z zakresu zabezpieczeń wirtualizacji:
Inicjatywa ta jest skoncentrowana na intensyfikacji świadomości oraz ekspansji umiejętności technicznych związanych z aspektami bezpieczeństwa operacyjnego w środowiskach wirtualizowanych. Program szkoleniowy został zaprojektowany tak, aby oferować kompendium wiedzy obejmujące kluczowe segmenty:
- Fundamenty Technologii Wirtualizacji: Wstępna część szkolenia dedykowana jest dogłębnemu zrozumieniu essencji technologii wirtualizacji, przybliżając uczestnikom szeroki wachlarz platform wirtualizacyjnych, w tym, lecz nie ograniczając się do, Vmware oraz Hyper-V. Uczestnicy zostaną zaznajomieni z kluczowymi funkcjami, możliwościami oraz praktycznymi zastosowaniami tych technologii w różnorodnych kontekstach biznesowych, uwydatniając ich strategiczne znaczenie dla nowoczesnych przedsiębiorstw.
- Konstrukcja, Konfiguracja i Administrowanie Maszynami Wirtualnymi: Ten moduł szkolenia skupia się na przekazaniu praktycznych wskazówek dotyczących procesów kreowania, konfiguracji oraz zarządzania wirtualnymi maszynami. Szczególny nacisk kładziony jest na procedury instalacji systemów operacyjnych, alokacji

zasobów oraz konfiguracji komunikacji sieciowej, z zamiarem maksymalizacji efektywności i wydajności wirtualnych środowisk operacyjnych.
- Metodologie Ochrony Infrastruktury Wirtualizowanej: Zaawansowany segment szkolenia poświęcony jest szczegółowej analizie i implementacji technik zabezpieczających infrastrukturę wirtualizowaną. Uczestnicy zgłębią metody i narzędzia umożliwiające izolację maszyn wirtualnych, zabezpieczanie hypervisorów oraz zarządzanie sieciami wirtualnymi, z naciskiem na kluczowe procedury monitorowania zagrożeń, konfigurację zasad zapór sieciowych oraz techniki segmentacji sieci wirtualnych. Omówione zostaną również zaawansowane strategie ochrony przed złośliwym oprogramowaniem i atakami sieciowymi, mające na celu zwiększenie odporności i bezpieczeństwa całego ekosystemu wirtualnego.
3. Szkolenie z zakresu bezpieczeństwa kopii zapasowych:
Inicjatywa szkoleniowa skoncentrowana na bezpieczeństwie kopii zapasowych kieruje się ku dogłębnemu zrozumieniu i praktycznej maestrii w zakresie kreowania oraz administracji bezpiecznymi mechanizmami backupu danych, akcentując na kluczowych komponentach:
- Fundamenty Backupu i Jego Znaczenie w Kontekście Bezpieczeństwa IT: Inauguracyjny moduł kursu dokonuje eksplikacji kluczowych pojęć i terminologii związanej z procesem tworzenia kopii zapasowych, podkreślając ich nieodzowną rolę w kompleksowej strategii bezpieczeństwa technologii informacyjnych oraz w zapewnieniu nieprzerwanej operacyjności korporacyjnych ekosystemów. Uczestnicy zdobywają perspektywę na istotę backupów jako niezbędnej linii obrony przed incydentami, które mogą zagrozić ciągłości działania organizacji.
- Dogłębna Analiza Typologii Kopii Zapasowych: Kurs prowadzi przez szczegółowe wyjaśnienie różnorodności form backupów – od pełnych, przez przyrostowe, aż po różnicowe – oferując równocześnie pragmatyczne wytyczne dotyczące ich efektywnego planowania, konfiguracji i implementacji. Omówienie to jest kluczowe dla zrozumienia optymalnych metod zarządzania cyklem życia danych oraz dla maksymalizacji efektywności procesów backupu.
- Implementacja Nowoczesnych Rozwiązań Backupowych: Ten segment szkolenia koncentruje się na adaptacji oraz wykorzystaniu zaawansowanych technologii i oprogramowania backupowego, włączając w to systemy lokalne oraz oparte na chmurze, techniki deduplikacji danych, mechanizmy kompresji oraz szyfrowania. Przedstawione zostają najnowsze narzędzia i metodologie, które umożliwiają zwiększenie efektywności i bezpieczeństwa procesów archiwizacji danych.
- Weryfikacja Efektywności Backupu i Strategii Odtwarzania: Kurs zawiera kompleksowe instrukcje dotyczące testowania efektywności tworzonych kopii zapasowych oraz procedur przywracania danych, z naciskiem na strategie prewencji i reagowania na kryzysy takie jak ataki ransomware. Uczestnicy uzyskują wiedzę na temat kluczowych praktyk i procedur testowych, które zapewniają gotowość na scenariusze awaryjne.
- Procedury i Strategie Odzyskiwania Danych po Awarii: Finalny moduł edukacyjny zagłębia się w omówienie metodyk
i praktycznych wytycznych szybkiego odzyskiwania funkcjonalności systemów po wystąpieniu incydentów. Szczególna uwaga poświęcona jest skutecznym strategiom odzyskiwania danych, które są fundamentem dla minimalizacji czasu przestoju i optymalizacji procesu odbudowy po awarii.
Podstawowym zamierzeniem niniejszego kursu szkoleniowego jest dostarczenie uczestnikom kompleksowego zestawu wiedzy teoretycznej oraz praktycznych kompetencji, które są krytyczne dla skutecznego administrowania i nadzorowania bezpieczeństwem infrastruktury technologicznej informacyjnej. Szczególny nacisk kładziony jest na głębokie zrozumienie i zarządzanie systemem Active Directory, ekosystemami wirtualizacji oraz złożonymi strategiami implementacji systemów kopii zapasowych. Celem tego szkolenia jest nie tylko przekroczenie granic czysto teoretycznego przekazu wiedzy, ale przede wszystkim rozwinięcie praktycznych umiejętności aplikacyjnych, które umożliwią uczestnikom efektywne zabezpieczanie wartościowych zasobów informatycznych przed rosnącą gamą zagrożeń cyfrowych oraz zagwarantowanie nieprzerwanej operacyjności systemów informatycznych.
Poprzez syntezę teoretycznych fundamentów z realnymi aplikacjami praktycznymi, program ma na celu wyekwipowanie uczestników w niezbędne narzędzia do identyfikacji, adekwatnej reakcji oraz neutralizacji potencjalnych zagrożeń bezpieczeństwa cyfrowego. Ponadto, kurs stawia za cel wdrożenie uczestników w głębinę najlepszych praktyk i standardów branżowych, które stanowią o kształcie profesjonalnej codziennej praktyki. Skupienie się na tych elementach ma kluczowe znaczenie dla kształtowania w uczestnikach umiejętności

nie tylko reaktywnych, ale przede wszystkim proaktywnych w kontekście zarządzania ryzykiem i ochrony infrastruktury IT. W rezultacie, program szkoleniowy ma na celu przygotowanie adeptów do pełnienia roli bastionu w obronie przed zagrożeniami, promując jednocześnie kulturę bezpieczeństwa informacyjnego, która jest fundamentem dla zrównoważonego rozwoju i innowacyjności w przestrzeni technologicznej organizacji.

32. Opracowanie i wdrożenie dokumentacji SZBI dla Urzędu oraz Ośrodka pomocy społecznej.

Cel Usługi:

Zasadniczym zamierzeniem proponowanej usługi jest kreacja kompleksowej, szczegółowo opracowanej dokumentacji dla Systemu Zarządzania Bezpieczeństwem Informacji (SZBI), która będzie w pełni zharmonizowana z międzynarodowymi normami i aktualnymi najlepszymi praktykami, przy jednoczesnym dostosowaniu do unikatowych aspektów i wymogów strukturalnych Zamawiającego. Celem jest, aby wspomniana dokumentacja służyła jako kluczowy fundament dla efektywnego implementowania, utrzymania oraz ciągłego udoskonalania SZBI, gwarantując tym samym wytrzymałość ochrony informacji wobec szerokiego spektrum potencjalnych zagrożeń oraz podnosząc poziom zaufania wśród interesariuszy.

Zakres Usługi:

1. Analiza Stanu Istniejącego i Określenie Wymagań:

- Realizacja audytu wstępnego mającego na celu szczegółową analizę obecnych procesów, procedur operacyjnych oraz mechanizmów kontroli związanych z bezpieczeństwem informacji, w celu zidentyfikowania istniejących luk i obszarów wymagających usprawnienia.
- Dokładna identyfikacja i agregacja wymagań prawnych, regulacyjnych oraz biznesowych dotyczących bezpieczeństwa informacji, aby zapewnić pełną zgodność przyszłego SZBI z obowiązującymi ramami normatywnymi.

2. Opracowanie Dokumentacji SZBI:

- Konstrukcja polityki bezpieczeństwa informacji, która będzie definiować kierunkowe cele, zakres działania, zasady oraz zakres odpowiedzialności w ramach struktury SZBI, stanowiąc podstawę dla wszystkich dalszych działań.
- Rozwój i formalizacja procedur, instrukcji operacyjnych, wytycznych oraz innych dokumentów kluczowych dla wdrożenia i efektywnego funkcjonowania SZBI, uwzględniając przy tym specyfikę organizacyjną Zamawiającego.

3. Weryfikacja i Walidacja Dokumentacji:

- Krytyczny przegląd i ocena zgodności opracowanej dokumentacji z międzynarodowymi standardami, wyznacznikami branżowymi oraz oczekiwaniami Zamawiającego, mający na celu zapewnienie jej maksymalnej adekwatności
i użyteczności.
- Organizacja warsztatów, konsultacji oraz sesji feedbackowych z kluczowymi stakeholderami organizacji, w celu osiągnięcia konsensusu co do finalnej formy i treści dokumentów.

4. Wsparcie przy Wdrożeniu Dokumentacji:

- Oferowanie doradztwa w zakresie implementacji najlepszych praktyk dotyczących wdrożenia procedur i polityk określonych w dokumentacji SZBI, z myślą o optymalizacji procesów bezpieczeństwa.
- Asystowanie w implementacji zaleceń oraz w organizacji szkoleń dla personelu, aby zapewnić im kompleksowe zrozumienie nowych procedur i polityk.

5. Przygotowanie do Certyfikacji:

- Dostosowanie dokumentacji do wymogów procesu certyfikacji według wybranych standardów, na przykład ISO/IEC 27001, co zapewni organizacji gotowość do podjęcia procedur weryfikacyjnych.

Cel Końcowy Usługi:

Finalizacja usługi zapewni Zamawiającemu kompleksową, spójną oraz w pełni funkcjonalną dokumentację SZBI, która stanie się solidnym fundamentem dla efektywnego zarządzania bezpieczeństwem informacji. Dzięki temu, organizacja uzyska dogłębne zrozumienie metod zarządzania ryzykiem, ochrony informacji oraz adaptacji do zmieniających się zagrożeń, co w konsekwencji umożliwi ciągłe doskonalenie systemu bezpieczeństwa informacji. Opracowana dokumentacja SZBI stanie się kluczowym elementem w strukturze zarządzania organizacją, zapewniając nie tylko zgodność z międzynarodowymi normami i najlepszymi praktykami, ale również dopasowanie do specyficznych wymogów i oczekiwań Zamawiającego.

I-I.271.11.2024 Gorzyce, 15.07.2024 r.

Dokumentacja ta będzie również służyć jako instrukcja operacyjna dla wszystkich pracowników i zainteresowanych stron, ułatwiając zrozumienie ich ról i odpowiedzialności w kontekście bezpieczeństwa informacji. W rezultacie, wszyscy uczestnicy procesu będą mieli jasne wytyczne dotyczące sposobu postępowania, co znacznie zwiększy ogólną świadomość bezpieczeństwa w organizacji oraz efektywność wdrażanych środków ochronnych.

Takie podejście zapewni organizacji nie tylko obronę przed potencjalnymi zagrożeniami, ale także pozytywnie wpłynie na reputację wśród klientów, partnerów biznesowych oraz innych interesariuszy, budując zaufanie poprzez demonstrację zaangażowania w ochronę poufnych informacji i danych osobowych. Finalnie, kompletna i zaktualizowana dokumentacja SZBI będzie stanowić nieoceniony zasób w procesie ciągłego monitorowania, przeglądania i ulepszania procesów bezpieczeństwa, umożliwiając organizacji dynamiczne reagowanie na nowe wyzwania i zapewniając stabilność operacyjną w zmieniającym się środowisku cyfrowym.

I-I.271.11.2024 Gorzyce, 15.07.2024 r.

Załącznik nr 3.
Zamawiający:
Gmina Gorzyce
ul. Sandomierska 75
389-432 Gorzyce

Oświadczenie Wykonawcy

OŚWIADCZENIE DOTYCZĄCE SPEŁNIANIA WARUNKÓW UDZIAŁU W POSTĘPOWANIU

Na potrzeby postępowania o udzielenie zamówienia publicznego pn.
Zakup sprzętu informatycznego, oprogramowania wraz ze szkoleniami i audytami w ramach konkursu grantowego Cyberbezpieczny Samorząd, oświadczam, co następuje:

OŚWIADCZENIE DOTYCZĄCE WYKONAWCY:

Oświadczam, że spełniam warunki udziału w postępowaniu określone przez Zamawiającego w Specyfikacji Warunków Zamówienia w rozdziale XX ust. 1.

INFORMACJA DOTYCZĄCA PODMIOTU, NA KTÓREGO ZASOBY POWOŁUJE SIĘ WYKONAWCA[3]:

Oświadczam, że w celu wykazania spełniania warunków udziału w postępowaniu, określonych przez Zamawiającego w Specyfikacji Warunków Zamówienia w rozdziale XX ust. 1.
zakresie:……..… polegam na zasobach następującego/ych podmiotu/ów: ……., w następującym zakresie: ……..…..…

(wskazać podmiot i określić odpowiedni zakres dla wskazanego podmiotu).

OŚWIADCZENIE DOTYCZĄCE PODANYCH INFORMACJI:

Oświadczam, że wszystkie informacje podane w powyższych oświadczeniach są aktualne i zgodne z prawdą oraz zostały przedstawione z pełną świadomością konsekwencji wprowadzenia Zamawiającego w błąd przy przedstawianiu informacji.

…….…… *(miejscowość),* dnia ……. r.

……
(podpis)

[3] Wypełnić jeżeli dotyczy

I-I.271.11.2024 Gorzyce, 15.07.2024 r.

Załącznik nr 4.
Zamawiający:
Gmina Gorzyce
ul. Sandomierska 75
389-432 Gorzyce

Oświadczenie Wykonawcy

OŚWIADCZENIE DOTYCZĄCE PRZESŁANEK WYKLUCZENIA Z POSTĘPOWANIA

Na potrzeby postępowania o udzielenie zamówienia publicznego pn.

Zakup sprzętu informatycznego, oprogramowania wraz ze szkoleniami i audytami w ramach konkursu grantowego Cyberbezpieczny Samorząd.

OŚWIADCZENIE DOTYCZĄCE WYKONAWCY:

Oświadczam, że nie podlegam wykluczeniu z postępowania na podstawie art. 108 ust. 1 Pzp.

……*(miejscowość),*dnia …… r.

……

(podpis)

Oświadczam, że zachodzą w stosunku do mnie podstawy wykluczenia z postępowania na podstawie art. …… ustawy Pzp *(podać mającą zastosowanie podstawę wykluczenia spośród wymienionych w art. 108 ust. 1).* Jednocześnie oświadczam, że w związku z ww. okolicznością, podjąłem następujące środki naprawcze:

……*

OŚWIADCZENIE DOTYCZĄCE PODMIOTU,

NA KTÓREGO ZASOBY POWOŁUJE SIĘ WYKONAWCA:

Oświadczam, że następujący/e podmiot/y, na którego/ych zasoby powołuję się w niniejszym postępowaniu, tj.:…… … *(podać pełną nazwę/firmę, adres, a także w zależności od podmiotu: NIP/PESEL)* nie podlega/ją wykluczeniu z postępowania o udzielenie zamówienia na podstawie art. 108 ust. 1 Pzp.

OŚWIADCZENIE DOTYCZĄCE PODWYKONAWCY

I-I.271.11.2024 Gorzyce, 15.07.2024 r.

NIEBĘDĄCEGO PODMIOTEM, NAKTÓREGO ZASOBY POWOŁUJE SIĘ WYKONAWCA:

Oświadczam, że następujący/e podmiot/y, będący/e podwykonawcą/ami: …… *(podać pełną nazwę/firmę, adres, a także w zależności od podmiotu: NIP/PESEL)*, nie podlega/ą wykluczeniu z postępowania o udzielenie zamówienia na podstawi art. 108 ust. 1 Pzp.

OŚWIADCZENIE DOTYCZĄCE PODANYCH INFORMACJI:

Oświadczam, że wszystkie informacje podane w powyższych oświadczeniach są aktualne i zgodne z prawdą oraz zostały przedstawione z pełną świadomością konsekwencji wprowadzenia Zamawiającego w błąd przy przedstawianiu informacji.

…… *(miejscowość),* dnia …… r.

……

(podpis)

*Wypełnić jeśli dotyczy

I-I.271.11.2024 Gorzyce, 15.07.2024 r.

Załącznik nr 5.
Zamawiający:
Gmina Gorzyce
ul. Sandomierska 75
39-432 Gorzyce

Oświadczenie Wykonawcy

OŚWIADCZENIE DOTYCZĄCE PRZYNALEŻNOŚCI LUB BRAKU PRZYNALEŻNOŚCI DO TEJ SAMEJ GRUPY KAPITAŁOWEJ I POTWIERDZAJĄCYM AKTUALNOŚĆ INFORMACJI ZAWARTYCH W OŚWIADCZENIU WSTĘPNYM.

Składając ofertę w przetargu na: ***Zakup sprzętu informatycznego, oprogramowania wraz ze szkoleniami i audytami w ramach konkursu grantowego Cyberbezpieczny Samorząd.***

Oświadczam/y, że wykonawca którego reprezentuję/emy

(należy zaznaczyć właściwe przy użyciu znaku np. „X")

☐ **NIE NALEŻY** z żadnym z wykonawców, którzy złożyli oferty w przedmiotowym postępowaniu do tej samej grupy kapitałowej, w rozumieniu ustawy z dnia 16 lutego 2007 r. o ochronie konkurencji i konsumentów,

☐ **NALEŻY do tej samej grupy kapitałowej***, w rozumieniu ustawy z dnia 16 lutego 2007 r. o ochronie konkurencji i konsumentów, razem z następującymi wykonawcami, którzy złożyli oferty w przedmiotowym postępowaniu:

……

……

……

Niniejszym potwierdzam aktualność informacji zawartych w oświadczeniu wstępnym złożonym w postępowaniu o udzielenie ww. zamówienia publicznego, na podstawie w art.125 ust. 1 ustawy Pzp, w zakresie braku podstaw wykluczenia z postępowania na podstawie art. 108 ust. 1.

……
(miejscowość i data)

……
(podpis)

Wraz ze złożeniem oświadczenia o przynależności do tej samej grupy kapitałowej, wykonawca składa dokumenty lub informacje potwierdzające przygotowanie oferty niezależnie od innego wykonawcy należącego do tej samej grupy kapitałowej.

I-I.271.11.2024 Gorzyce, 15.07.2024 r.

Załącznik nr 6.
Zamawiający:
Gmina Gorzyce
ul. Sandomierska 75
39-432 Gorzyce

Zobowiązanie podmiotu trzeciego

do oddania do dyspozycji Wykonawcy niezbędnych zasobów na okres korzystania z nich przy wykonywaniu zamówienia wraz z oświadczeniem o niepodleganiu odrzuceniu oraz spełnienia warunków zamówienia.

W imieniu:

_____

(wpisać nazwę Podmiotu, na zasobach którego polega Wykonawca)

Zobowiązuję się do oddania swoich zasobów

_____

(określenie zasobu – zdolność techniczna, zdolność zawodowa)

do dyspozycji Wykonawcy:

_____

(wpisać nazwę Wykonawcy)

przy wykonywaniu zamówienia pn. ***„……”.***

Oświadczam, iż:
1) udostępniam Wykonawcy w/w zasoby, w następującym zakresie:

I-I.271.11.2024 Gorzyce, 15.07.2024 r.

……

2) sposób wykorzystania udostępnionych przeze mnie zasobów będzie następujący:
……

3) zakres mojego udziału przy wykonywaniu zamówienia będzie następujący:
……

4) okres mojego udziału przy wykonywaniu zamówienia będzie następujący:
……

5) udostępniając wykonawcy zdolności w postaci wykształcenia, kwalifikacji zawodowych lub doświadczenia będę realizował roboty budowlane, których dotyczą udostępnione zdolności:
TAK*/NIE *

UWAGA:
Zamiast niniejszego Formularza można przedstawić inne dokumenty, w szczególności:
1) pisemne zobowiązanie podmiotu, o którym mowa w art. 118 ustawy Pzp,
2) dokumenty dotyczące:
a. zakresu dostępnych wykonawcy zasobów innego podmiotu;
b. sposobu wykorzystania zasobów innego podmiotu, przez Wykonawcę przy wykonywaniu zamówienia publicznego;
c. zakresu i okresu udziału innego podmiotu przy wykonywaniu zamówienia;
d. czy podmiot, na zdolnościach którego wykonawca polega w odniesieniu do warunków udziału w postępowaniu dotyczących wykształcenia, kwalifikacji zawodowych lub doświadczenia, zrealizuje roboty budowalne, których wskazane zdolności dotyczą.

Ponadto poniżej składam następujące oświadczenia:

I. <u>DOTYCZĄCE PRZESŁANEK WYKLUCZENIA Z POSTĘPOWANIA</u>

1) Oświadczam, że nie podlegam wykluczeniu z postępowania na podstawie art. 108 ust. 1 ustawy Pzp.
2) Oświadczam, że zachodzą w stosunku do mnie podstawy wykluczenia z postępowania na podstawie art. ……. ustawy Pzp *(podać mającą zastosowanie podstawę wykluczenia spośród wymienionych w art. 108 ust. 1 ustawy Pzp).* Jednocześnie oświadczam, że w związku z ww. okolicznością, na podstawie art. 110 ust 2 ustawy Pzp podjąłem następujące środki naprawcze:
……
……

II. <u>DOTYCZĄCE SPEŁNIANIA WARUNKÓW UDZIAŁU W POSTĘPOWANIU</u>
Oświadczam, że spełniam warunki udziału w postępowaniu określone w specyfikacji warunków zamówienia w zakresie, w jakim Wykonawca powołuje się na te zasoby.

I-I.271.11.2024 Gorzyce, 15.07.2024 r.

III. OŚWIADCZENIE DOTYCZĄCE PODANYCH INFORMACJI:

Oświadczam, że wszystkie informacje podane w powyższych oświadczeniach są aktualne i zgodne z prawdą oraz zostały przedstawione z pełną świadomością konsekwencji wprowadzenia zamawiającego w błąd przy przedstawianiu informacji.

…… *(miejscowość),* dnia ……. r.

……

(podpis)

_____

* - *niepotrzebne skreślić*

I-I.271.11.2024 Gorzyce, 15.07.2024 r.

Załącznik nr 7.
Zamawiający:
Gmina Gorzyce
ul. Sandomierska 75
39-432 Gorzyce

O Ś W I A D C Z E N I E

składane na podstawie art. 117 ust. 4 ustawy Prawo zamówień publicznych

dla Wykonawców ubiegających się wspólnie o udzielenie zamówienia publicznego

Przystępując do udziału w postępowaniu o udzielenie zamówienia publicznego w trybie podstawowym, o jakim stanowi art. 275 pkt 1 Pzp, prowadzonego na podstawie ustawy z dnia 11 września 2019 r. Prawo zamówień publicznych (Dz. U. z 2019 r., poz. 2019 z późn. zm. – *zwana dalej Pzp),* którego przedmiotem jest ***Zakup sprzętu informatycznego, oprogramowania wraz ze szkoleniami i audytami w ramach konkursu grantowego Cyberbezpieczny Samorząd*** na podstawie art. 117 ust. 4 Pzp oświadczam/y, że poszczególni wykonawcy zrealizują następujące usługi/roboty:

Lp.	Nazwa Wykonawcy	Wykonywana usługa w ramach realizacji zamówienia
1.		
2		
3.		

…… *(miejscowość),* dnia …… r.

……

(podpis)

I-I.271.11.2024 Gorzyce, 15.07.2024 r.

Załącznik nr 8

Zamawiający:

Gmina Gorzyce
ul. Sandomierska 75
39-432 Gorzyce

OŚWIADCZENIE WYKONAWCY DOTYCZĄCE PRZESŁANEK WYKLUCZENIA Z ART. 7 UST. 1 USTAWY O SZCZEGÓLNYCH ROZWIĄZANIACH W ZAKRESIE PRZECIWDZIAŁANIA WSPIERANIU AGRESJI NA UKRAINĘ ORAZ SŁUŻĄCYCH OCHRONIE BEZPIECZEŃSTWA NARODOWEGO

W związku ze złożeniem oferty w postępowaniu o udzielenie zamówienia publicznego prowadzonym w trybie przetargu nieograniczonego pn. ***Zakup sprzętu informatycznego, oprogramowania wraz ze szkoleniami i audytami w ramach konkursu grantowego Cyberbezpieczny Samorząd.***

Ja niżej podpisany:

……

działając w imieniu i na rzecz:

……

1. Oświadczam, że nie zachodzą w stosunku do mnie przesłanki wykluczenia z postępowania na podstawie art. 7 ust. 1 ustawy z dnia 13 kwietnia 2022 r. o szczególnych rozwiązaniach w zakresie przeciwdziałania wspieraniu agresji na Ukrainę oraz służących ochronie bezpieczeństwa narodowego (Dz. U. z 2023 r. poz.1497).[4]

[4] Zgodnie z treścią art. 7 ust. 1 ustawy z dnia 13 kwietnia 2022 r. *o szczególnych rozwiązaniach w zakresie przeciwdziałania wspieraniu agresji na Ukrainę oraz służących ochronie bezpieczeństwa narodowego,* z postępowania o udzielenie zamówienia publicznego lub konkursu prowadzonego na podstawie ustawy Pzp wyklucza się:
1) wykonawcę oraz uczestnika konkursu wymienionego w wykazach określonych w rozporządzeniu 765/2006 i rozporządzeniu 269/2014 albo wpisanego na listę na podstawie decyzji w sprawie wpisu na listę rozstrzygającej o zastosowaniu środka, o którym mowa w art. 1 pkt 3 ustawy;
2) wykonawcę oraz uczestnika konkursu, którego beneficjentem rzeczywistym w rozumieniu ustawy z dnia 1 marca 2018 r. o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu (Dz. U. z 2022 r. poz. 593 i 655) jest osoba wymieniona w wykazach określonych w rozporządzeniu 765/2006 i rozporządzeniu 269/2014 albo wpisana na listę lub będąca takim beneficjentem rzeczywistym od dnia 24 lutego 2022 r., o ile została wpisana na listę na podstawie decyzji w sprawie wpisu na listę rozstrzygającej o zastosowaniu środka, o którym mowa w art. 1 pkt 3 ustawy;
3) wykonawcę oraz uczestnika konkursu, którego jednostką dominującą w rozumieniu art. 3 ust. 1 pkt 37 ustawy z dnia 29 września 1994 r. o rachunkowości (Dz. U. z 2021 r. poz. 217, 2105 i 2106), jest podmiot wymieniony w wykazach określonych w rozporządzeniu 765/2006 i rozporządzeniu 269/2014 albo wpisany na listę lub będący taką jednostką dominującą od dnia 24 lutego 2022 r., o ile został wpisany na listę na podstawie decyzji w sprawie wpisu na listę rozstrzygającej o zastosowaniu środka, o którym mowa w art. 1 pkt 3 ustawy.

Klauzula informacyjna z art. 13 RODO do zastosowania przez zamawiających w celu związanym z postępowaniem o udzielenie zamówienia publicznego

Zgodnie z art. 13 ust. 1 i 2 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz. Urz. UE L 119 z 04.05.2016, str. 1), dalej „RODO", informuję, że:

- administratorem Pani/Pana danych osobowych jest *Gmina Gorzyce, ul. Sandomierska 75, 39-432 Gorzyce;*
- inspektor ochrony danych osobowych w *Gminie Gorzyce - iodo@gminagorzyce.pl, tel. 15 83 62 075*;
- Pani/Pana dane osobowe przetwarzane będą na podstawie art. 6 ust. 1 lit. c RODO w celu związanym z postępowaniem o udzielenie zamówienia publicznego prowadzonym w trybie przetargu nieograniczonego;
- odbiorcami Pani/Pana danych osobowych będą osoby lub podmioty, którym udostępniona zostanie dokumentacja postępowania w oparciu o art. 16, art. 18 oraz art. 71 ustawy z dnia 11 września 2019 roku Prawo zamówień publicznych (Dz. U. 2019, poz. 2019), dalej „ustawa Pzp";
- Pani/Pana dane osobowe będą przechowywane, zgodnie z art. 78 ust. 1 ustawy Pzp, przez okres 4 lat od dnia zakończenia postępowania o udzielenie zamówienia, a jeżeli czas trwania umowy przekracza 4 lata, okres przechowywania obejmuje cały czas trwania umowy;
- obowiązek podania przez Panią/Pana danych osobowych bezpośrednio Pani/Pana dotyczących jest wymogiem ustawowym określonym w przepisach ustawy Pzp, związanym z udziałem w postępowaniu o udzielenie zamówienia publicznego; konsekwencje niepodania określonych danych wynikają z ustawy Pzp;
- w odniesieniu do Pani/Pana danych osobowych decyzje nie będą podejmowane w sposób zautomatyzowany, stosowanie do art. 22 RODO;
- posiada Pani/Pan:
  - na podstawie art. 15 RODO prawo dostępu do danych osobowych Pani/Pana dotyczących;
  - na podstawie art. 16 RODO prawo do sprostowania Pani/Pana danych osobowych **;
  - na podstawie art. 18 RODO prawo żądania od administratora ograniczenia przetwarzania danych osobowych z zastrzeżeniem przypadków, o których mowa w art. 18 ust. 2 RODO ***;
  - prawo do wniesienia skargi do Prezesa Urzędu Ochrony Danych Osobowych, gdy uzna Pani/Pan, że przetwarzanie danych osobowych Pani/Pana dotyczących narusza przepisy RODO;
- nie przysługuje Pani/Panu:
  - w związku z art. 17 ust. 3 lit. b, d lub e RODO prawo do usunięcia danych osobowych;

- prawo do przenoszenia danych osobowych, o którym mowa w art. 20 RODO;
- na podstawie art. 21 RODO prawo sprzeciwu, wobec przetwarzania danych osobowych, gdyż podstawą prawną przetwarzania Pani/Pana danych osobowych jest art. 6 ust. 1 lit. c RODO.