Załącznik nr 1 do zapytania ofertowego

SZCZEGÓŁOWY OPIS PRZEDMIOTU ZAMÓWIENIA

Dostawa, wdrożenie, konfiguracja oraz utrzymanie urządzeń i oprogramowania z zakresu cyberbezpieczeństwa dla Gminy Kowal

w ramach Projektu „Cyberbezpieczna Gmina Kowal” dofinansowanego ze środków Unii Europejskiej w ramach konkursu grantowego „Cyberbezpieczny Samorząd” realizowanego w ramach Funduszy Europejskich na Rozwój Cyfrowy 2021-2027 (FERC) Priorytet II: Zaawansowane usługi cyfrowe. Działanie 2.2. – Wzmocnienie krajowego systemu cyberbezpieczeństwa.

Fundusze Europejskie na Rozwój Cyfrowy
Rzeczpospolita Polska
Dofinansowane przez Unię Europejską
CENTRUM PROJEKTÓW POLSKA CYFROWA

SPIS TREŚCI

1. [WS] WSTĘP

W ramach załącznika przedstawiono wymagania dotyczące opisu przedmiotu zamówienia: "Dostawa, wdrożenie, konfiguracja oraz utrzymanie urządzeń i oprogramowania z zakresu cyberbezpieczeństwa dla Gminy Kowal".

W ramach dokumentu użyto następujących typów wymagalności parametrów technicznych i funkcjonalnych:
- "MUSI BYĆ" - brak spełnienia wymagania może stanowić podstawę do odrzucenia oferty lub rozwiązania umowy na każdym etapie realizacji zamówienia,
- "OPCJONALNE" - brak spełnienia wymagania nie stanowi podstawy do odrzucenia oferty,
- "PUNKTOWANE" - spełnienie wymagania stanowi podstawę do naliczenia dodatkowych punktów na etapie oceny ofert zgodnie z kryteriami określonymi w postępowaniu.

Zamawiający informuje, że wszelkie wskazane w OPZ wymagania dotyczące niniejszego postępowania, w szczególności: normy, specyfikacje techniczne, nazwy własne, numery katalogowe, znaki towarowe, patenty lub pochodzenie, źródła lub szczególne procesy, które charakteryzują produkty lub usługi dostarczane przez konkretnego wykonawcę, mają charakter przykładowy.
Zostały one przywołane jedynie w celu sprecyzowania parametrów i wymogów techniczno-użytkowych przedmiotu zamówienia, Zamawiający dopuszcza materiały, urządzenia i technologie równoważne.
Wszelkie materiały, urządzenia i rozwiązania równoważne, muszą spełniać następujące wymagania i standardy w stosunku do oprogramowania, urządzenia i rozwiązania wskazanego jako przykładowy, tj. muszą być co najmniej:
1. tego samego charakteru użytkowego (tożsamość funkcji),
2. tej samej charakterystyki materiałowej (rodzaj i jakość materiałów),
3. tych samych parametrów technicznych (wytrzymałość, trwałość, itp);
4. tych samych parametrów bezpieczeństwa użytkowania;
oraz muszą być
5. kompatybilne z istniejącą infrastrukturą Zamawiającego,
6. spełniać te same funkcje,
7. posiadać stosowne dokumenty dopuszczające do stosowania certyfikaty, atesty i aprobaty techniczne.
Zastosowanie rozwiązań równoważnych nie może prowadzić do pogorszenia właściwości przedmiotu zamówienia.

Zamówienie powinno zostać zrealizowane z uwzględnieniem wymagań technicznych i funkcjonalnych opisanych w poniższych rozdziałach, które należy traktować jako minimalne parametry do rozwiązań równoważnych.

2. [GKUTM] WYMAGANIA TECHNICZNE W ZAKRESIE ROUTERA BRZEGOWEGO UTM

W ramach tego podzadania ma być wykonana dostawa i instalacja 2 szt. routerów brzegowych UTM zabezpieczających łącza internetowe dla GOPS i ZSPG. Router posiada następujące minimalne lub równoważne parametry:

Lp.	ID	Nazwa wymagania	Wymagalność
2.1.	GKUTM_001	Typ obudowy: Wysokość pojedynczego urządzenia maksymalnie 1U.	MUSI BYĆ
2.2.	GKUTM_002	System bezpieczeństwa realizuje wszystkie wymienione poniżej funkcje sieciowe i bezpieczeństwa niezależnie od dostawcy łącza.	MUSI BYĆ
2.3.	GKUTM_003	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.	MUSI BYĆ
2.4.	GKUTM_004	Dla wszystkich funkcji systemu wymagane jest dostarczenie dokumentu potwierdzonego przez producenta lub autoryzowanego dystrybutora o gotowości świadczenia usług wsparcia w języku polskim oraz bezpłatnej obsługi procesu wymiany uszkodzonego urządzenia.	MUSI BYĆ
2.5.	GKUTM_005	System realizujący funkcję Firewall zapewnia pracę w jednym z trzech trybów: Routera z funkcją NAT, transparentnym oraz monitorowania na porcie SPAN.	MUSI BYĆ
2.6.	GKUTM_006	System umożliwia budowę minimum 2 oddzielnych (fizycznych lub logicznych) instancji systemów w zakresie: Routingu, Firewall'a, IPSec VPN, Antywirus, IPS, Kontroli Aplikacji.	MUSI BYĆ
2.7.	GKUTM_007	Istnieje możliwość dedykowania co najmniej 4 administratorów do poszczególnych instancji systemu.	MUSI BYĆ
2.8.	GKUTM_008	System wspiera protokoły IPv4 oraz IPv6 w zakresie: a) Firewall. b) Ochrony w warstwie aplikacji. c) Protokołów routingu dynamicznego.	MUSI BYĆ
2.9.	GKUTM_009	Wymagania techniczne w zakresie redundancji, monitoringu i wykrywania awarii: a) System ma możliwość pracy w postaci redundantnego klastra. b) 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. c) Możliwość monitorowania i wykrywania uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łączy sieciowych. d) Możliwość monitorowania stanu realizowanych połączeń VPN. e) Możliwość agregacji linków statyczną oraz w oparciu o protokół LACP. f) Możliwość tworzenia interfejsów redundantnych.	MUSI BYĆ
2.10.	GKUTM_010	Wymagania techniczne w zakresie interfejsów, dysku i zasilania: a) System realizujący funkcję Firewall dysponuje co najmniej poniższą liczbą i rodzajem interfejsów: - Porty RJ-45 1Gbps – min. 6 szt. - Porty RJ-45 1Gbps dedykowane do połączenia ze switchem – min. 2 szt. - Porty współdzielone WAN RJ-45/SFP – min. 2 szt. b) System Firewall posiada wbudowany port konsoli szeregowej oraz gniazdo USB umożliwiające podłączenie modemu 3G/4G oraz instalacji oprogramowania z klucza USB.	MUSI BYĆ

Fundusze Europejskie na Rozwój Cyfrowy | Rzeczpospolita Polska | Dofinansowane przez Unię Europejską | Centrum Projektów Polska Cyfrowa

Lp.	ID	Nazwa wymagania	Wymagalność
2.11.	GKUTM_011	Wymagania techniczne w zakresie parametrów wydajnościowych: a) Obsługa nie mniej niż 1,5 mln jednoczesnych połączeń TCP oraz 45 tys. nowych połączeń TCP na sekundę. b) Przepustowość IPv4 Firewall: nie mniej niż 10 Gbps dla pakietów UDP 512 B. c) Przepustowość Firewall z włączoną funkcją Kontroli Aplikacji: nie mniej niż 1,8 Gbps.	MUSI BYĆ
2.12.	GKUTM_012	Wymagania techniczne w zakresie funkcji systemu bezpieczeństwa: a) Kontrola dostępu - zapora ogniowa klasy Stateful Inspection. b) Kontrola Aplikacji. c) Poufność transmisji danych - połączenia szyfrowane IPSec VPN oraz SSL VPN. d) Ochrona przed malware. e) Ochrona przed atakami - Intrusion Prevention System. f) Kontrola stron WWW. g) Kontrola zawartości poczty – Antyspam dla protokołów SMTP, POP3. h) Zarządzanie pasmem (QoS, Traffic shaping). i) Mechanizmy ochrony przed wyciekiem poufnej informacji (DLP). j) 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. k) Inspekcja (minimum: IPS) ruchu szyfrowanego protokołem SSL/TLS, minimum dla następujących typów ruchu: HTTP (w tym HTTP/2), SMTP, FTP, POP3. l) Funkcja lokalnego serwera DNS z możliwością filtrowania zapytań DNS na lokalnym serwerze DNS jak i w ruchu przechodzącym przez system. m) 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).	MUSI BYĆ
2.13.	GKUTM_013	Wymagania techniczne w zakresie polityk firewall: a) Polityka Firewall uwzględnia: adresy IP, użytkowników, protokoły, usługi sieciowe, aplikacje lub zbiory aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń. b) 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. c) W ramach systemu istnieje możliwość tworzenia wydzielonych stref bezpieczeństwa np. DMZ, LAN, WAN. d) Możliwość wykorzystania w polityce bezpieczeństwa zewnętrznych repozytoriów zawierających: kategorie URL, adresy IP. e) Polityka firewall umożliwia filtrowanie ruchu w zależności od kraju, do którego przypisane są adresy IP źródłowe lub docelowe. f) Możliwość ustawienia przedziału czasu, w którym dana reguła w politykach firewall jest aktywna. g) 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.	MUSI BYĆ

Lp.	ID	Nazwa wymagania	Wymagalność
2.14.	GKUTM_014	System umożliwia konfigurację połączeń typu IPSec VPN. W zakresie tej funkcji zapewnia: a) Wsparcie dla IKE v1 oraz v2. b) Obsługę szyfrowania protokołem minimum AES z kluczem 128 oraz 256 bitów w trybie pracy Galois/Counter Mode(GCM). c) Obsługa protokołu Diffie-Hellman grup 19, 20. d) Wsparcie dla Pracy w topologii Hub and Spoke oraz Mesh. e) Tworzenie połączeń typu Site-to-Site oraz Client-to-Site. f) Monitorowanie stanu tuneli VPN i stałego utrzymywania ich aktywności. g) Możliwość wyboru tunelu przez protokoły: dynamicznego routingu (np. OSPF) oraz routingu statycznego. h) Wsparcie dla następujących typów uwierzytelniania: pre-shared key, certyfikat. i) Możliwość ustawienia maksymalnej liczby tuneli IPSec negocjowanych (nawiązywanych) jednocześnie w celu ochrony zasobów systemu. j) Możliwość monitorowania wybranego tunelu IPSec site-to-site i w przypadku jego niedostępności automatycznego aktywowania zapasowego tunelu. k) Obsługę mechanizmów: IPSec NAT Traversal, DPD, Xauth. l) Mechanizm „Split tunneling” dla połączeń Client-to-Site.	MUSI BYĆ
2.15.	GKUTM_015	System umożliwia konfigurację połączeń typu SSL VPN. W zakresie tej funkcji zapewnia: a) 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. b) Pracę w trybie Tunnel z możliwością włączenia funkcji „Split tunneling” przy zastosowaniu dedykowanego klienta. c) 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.	MUSI BYĆ
2.16.	GKUTM_016	Wymagania techniczne w zakresie routingu i obsługi łączy WAN: a) Obsługa routingu statycznego. b) Obsługa Policy Based Routingu (w tym: wybór trasy w zależności od adresu źródłowego, protokołu sieciowego, oznaczeń Type of Service w nagłówkach IP). c) Obsługa protokołów dynamicznego routingu w oparciu o protokoły: RIPv2 (w tym RIPng), OSPF (w tym OSPFv3), BGP oraz PIM. d) Możliwość filtrowania tras rozgłaszanych w protokołach dynamicznego routingu. e) Obsługa ECMP (Equal cost multi-path) – wybór wielu równoważnych tras w tablicy routingu. f) Obsługa BFD (Bidirectional Forwarding Detection). g) Obsługa monitoringu dostępności wybranego adresu IP z danego interfejsu urządzenia i w przypadku jego niedostępności automatyczne usunięcie wybranych tras z tablicy routingu.	MUSI BYĆ
2.17.	GKUTM_017	Wymagania techniczne w zakresie funkcji SD-WAN: a) System umożliwia wykorzystanie protokołów dynamicznego routingu przy konfiguracji równoważenia obciążenia do łączy WAN. b) SD-WAN wspiera zarówno interfejsy fizyczne jak i wirtualne (w tym VLAN, IPSec).	MUSI BYĆ
2.18.	GKUTM_018	Wymagania techniczne w zakresie zarządzania pasmem: a) System Firewall umożliwia zarządzanie pasmem poprzez określenie: maksymalnej i gwarantowanej ilości pasma, oznaczanie DSCP oraz wskazanie priorytetu ruchu. b) System daje możliwość określania pasma dla poszczególnych aplikacji. c) System pozwala zdefiniować pasmo dla wybranych użytkowników niezależnie od ich adresu IP. d) System zapewnia możliwość zarządzania pasmem dla wybranych kategorii URL.	MUSI BYĆ

Lp.	ID	Nazwa wymagania	Wymagalność
2.19.	GKUTM_019	Wymagania techniczne w zakresie ochrony przed malware: a) Silnik antywirusowy umożliwia skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021). b) Silnik antywirusowy zapewnia skanowanie następujących protokołów: HTTP, HTTPS, FTP, POP3, IMAP, SMTP, CIFS. c) 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. d) System umożliwia blokowanie i logowanie archiwów, które nie mogą zostać przeskanowane, ponieważ są zaszyfrowane, uszkodzone lub system nie wspiera inspekcji tego typu archiwów. e) System dysponuje sygnaturami do ochrony urządzeń mobilnych (co najmniej dla systemu operacyjnego Android). f) Baza sygnatur jest aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora. g) 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. h) System zapewnia usuwanie aktywnej zawartości plików PDF oraz Microsoft Office bez konieczności blokowania transferu całych plików. i) Możliwość wykorzystania silnika sztucznej inteligencji AI wytrenowanego przez laboratoria producenta. j) Możliwość uruchomienia ochrony przed malware dla wybranego zakresu ruchu.	MUSI BYĆ
2.20.	GKUTM_020	Wymagania techniczne w zakresie ochrony przed atakami: a) Ochrona IPS opiera się co najmniej na analizie sygnaturowej oraz na analizie anomalii w protokołach sieciowych. b) System chroni przed atakami na aplikacje pracujące na niestandardowych portach. c) Administrator systemu ma możliwość definiowania własnych wyjątków oraz własnych sygnatur. d) System zapewnia wykrywanie anomalii protokołów i ruchu sieciowego, realizując tym samym podstawową ochronę przed atakami typu DoS oraz DDoS. e) Mechanizmy ochrony dla aplikacji Web'owych na poziomie sygnaturowym (co najmniej ochrona przed: CSS, SQL Injecton, Trojany, Exploity, Roboty). f) Możliwość kontrolowania długości nagłówka, ilości parametrów URL oraz Cookies dla protokołu http. g) Wykrywanie i blokowanie komunikacji C&C do sieci botnet. h) Możliwość uruchomienia ochrony przed atakami dla wybranych zakresów komunikacji sieciowej. Mechanizmy ochrony IPS nie mogą działać globalnie.	MUSI BYĆ

Lp.	ID	Nazwa wymagania	Wymagalność
2.21.	GKUTM_021	Wymagania techniczne w zakresie kontroli aplikacji: a) Funkcja Kontroli Aplikacji umożliwia kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP. b) Baza Kontroli Aplikacji jest aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora. c) Aplikacje chmurowe (co najmniej: Facebook, Google Docs, Dropbox) są kontrolowane pod względem wykonywanych czynności, np.: pobieranie, wysyłanie plików. d) Baza sygnatur zawiera kategorie aplikacji szczególnie istotne z punktu widzenia bezpieczeństwa: proxy, P2P. e) Administrator systemu ma możliwość definiowania wyjątków oraz własnych sygnatur. f) Istnieje możliwość blokowania aplikacji działających na niestandardowych portach (np. FTP na porcie 2021). g) 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).	MUSI BYĆ
2.22.	GKUTM_022	Wymagania techniczne w zakresie kontroli WWW: a) Moduł kontroli WWW korzysta z bazy zawierającej co najmniej 40 milionów adresów URL pogrupowanych w kategorie tematyczne. b) 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. c) Filtr WWW dostarcza kategorii stron zabronionych prawem np.: Hazard. d) Administrator ma możliwość nadpisywania kategorii oraz tworzenia wyjątków – białe/czarne listy dla adresów URL. e) Filtr WWW umożliwia statyczne dopuszczanie lub blokowanie ruchu do wybranych stron WWW, w tym pozwala definiować strony z zastosowaniem wyrażeń regularnych (Regex). f) Filtr WWW daje możliwość wykonania akcji typu „Warning” – ostrzeżenie użytkownika wymagające od niego potwierdzenia przed otwarciem żądanej strony. g) Funkcja Safe Search – przeciwdziałająca pojawieniu się niechcianych treści w wynikach wyszukiwarek takich jak: Google oraz Yahoo. h) Administrator ma możliwość definiowania komunikatów zwracanych użytkownikowi dla różnych akcji podejmowanych przez moduł filtrowania WWW. i) System pozwala określić, dla których kategorii URL lub wskazanych URL nie będzie realizowana inspekcja szyfrowanej komunikacji.	MUSI BYĆ
2.23.	GKUTM_023	Wymagania techniczne w zakresie funkcji uwierzytelniania użytkowników w ramach sesji: a) 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. b) System daje możliwość zastosowania w tym procesie uwierzytelniania dwuskładnikowego. c) 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. d) Uwierzytelnianie w oparciu o protokół SAML w politykach bezpieczeństwa systemu dotyczących ruchu HTTP.	MUSI BYĆ

Lp.	ID	Nazwa wymagania	Wymagalność
2.24.	GKUTM_024	Wymagania techniczne w zakresie zarządzania: a) Elementy systemu bezpieczeństwa mają możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH, jak i mogą współpracować z dedykowanymi platformami centralnego zarządzania i monitorowania. b) Komunikacja elementów systemu zabezpieczeń z platformami centralnego zarządzania jest realizowana z wykorzystaniem szyfrowanych protokołów. c) Możliwość włączenia mechanizmów uwierzytelniania dwu-składnikowego dla dostępu administracyjnego. d) System współpracuje z rozwiązaniami monitorowania poprzez protokoły SNMP w wersjach 2c, 3 oraz umożliwia przekazywanie statystyk ruchu za pomocą protokołów Netflow lub sFlow. e) Możliwość zarządzania przez systemy firm trzecich poprzez API, do którego producent udostępnia dokumentację. f) Element systemu pełniący funkcję Firewall posiada wbudowane narzędzia diagnostyczne, przynajmniej: ping, traceroute, podglądu pakietów, monitorowanie procesowania sesji oraz stanu sesji firewall. g) Element systemu realizujący funkcję Firewall umożliwia wykonanie szeregu zmian przez administratora w CLI lub GUI, które nie zostaną zaimplementowane zanim nie zostaną zatwierdzone. h) Możliwość przypisywania administratorom praw do zarządzania określonymi częściami systemu (RBM). i) Możliwość zarządzania systemem tylko z określonych adresów źródłowych IP.	MUSI BYĆ
2.25.	GKUTM_025	Wymagania techniczne w zakresie logowania: a) 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. b) 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. c) Logowanie obejmuje zdarzenia dotyczące wszystkich modułów sieciowych i bezpieczeństwa. d) Możliwość włączenia logowania per reguła w polityce firewall. e) System zapewnia możliwość logowania do serwera SYSLOG. f) Przesyłanie SYSLOG do zewnętrznych systemów jest możliwe z wykorzystaniem protokołu TCP oraz szyfrowania SSL/TLS.	MUSI BYĆ
2.26.	GKUTM_026	Dostarczone subskrypcje na okres do 01 maja 2026. Subskrypcja ma upoważniać Zamawiającego do korzystania z aktualnych baz funkcji ochronnych producenta i serwisów. Powinna ona obejmować: a) Ochrona przed atakami - Intrusion Prevention System b) Ochrona przed malware c) Kontrola aplikacji d) Kontrola stron WWW e) Kontrola zawartości poczty	MUSI BYĆ
2.27.	GKUTM_027	Gwarancja 24 miesiące. UTM jest objęty serwisem gwarancyjnym producenta realizowanym na terenie Rzeczpospolitej Polskiej, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości. W przypadku gdy producent nie posiada na terenie Rzeczpospolitej Polskiej własnego centrum serwisowego, oferent winien przedłożyć dokument producenta, który wskazuje podmiot uprawniony do realizowania serwisu gwarancyjnego na terenie Rzeczpospolitej Polskiej. W ramach tego serwisu producent zapewnia również dostęp do aktualizacji oprogramowania oraz wsparcie techniczne w trybie 24x7.	MUSI BYĆ

Lp.	ID	Nazwa wymagania	Wymagalność
2.28.	GKUTM_028	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. Obsługa zgłoszenia w tym zwrot uszkodzonego urządzenia do producenta, bez dodatkowych kosztów po stronie zamawiającego, realizowana przez producenta lub autoryzowanego dystrybutora w języku polskim przez okres wymaganej gwarancji.	MUSI BYĆ
2.29.	GKUTM_029	Opisy do wymagań ogólnych a) 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.). b) Zamawiający wymaga oświadczenie producenta lub autoryzowanego dystrybutora producenta na terenie Polski, iż produkt pochodzi z autoryzowanego kanału sprzedaży, np. poprzez oświadczenie o posiadanym statusie autoryzacyjnym.	MUSI BYĆ
2.30.	GKUTM_030	Oferent winien przedłożyć dokumenty: a) Oświadczanie Producenta lub Autoryzowanego Dystrybutora świadczącego wsparcie techniczne o gotowości świadczenia na rzecz Zamawiającego wymaganego serwisu (zawierające: adres strony internetowej serwisu i numer infolinii telefonicznej). b) Certyfikat ISO 9001 podmiotu serwisującego.	MUSI BYĆ

3. [GKSD] WYMAGANIA TECHNICZNE W ZAKRESIE SERWERA DO WYKONYWANIA KOPII ZAPASOWYCH Z MECHANIZMEM DEDUPLIKACJI DANYCH

W ramach tego podzadania ma być wykonana dostawa i instalacja 1 szt. serwera do wykonywania kopii zapasowych z mechanizmem deduplikacji danych dla UGK. Serwer posiada następujące minimalne lub równoważne parametry:

Lp.	ID	Nazwa wymagania	Wymagalność
3.1.	GKSD_001	Urządzenie jest przeznaczone do deduplikacji i przechowywania kopii zapasowych.	MUSI BYĆ
3.2.	GKSD_002	Urządzenie oferuje przestrzeń min. 8TB netto powierzchni użytkowej bez uwzględniania mechanizmów protekcji. Wymagana możliwość czterokrotnego zwiększenia pojemności netto w obrębie tego samego urządzenia (przy zachowaniu globalnej deduplikacji w obrębie całej dostępnej przestrzeni dedykowanej do składowania danych)	MUSI BYĆ
3.3.	GKSD_003	Urządzenie posiada minimum: a) 4 porty Eth 10Gb/s Base-T RJ-45 b) 2 porty Eth 10Gb/s SFP+ wraz z wkładkami Wymagana możliwość obsługi każdym portem Ethernet protokołów CIFS, NFS, deduplikacja na źródle.	MUSI BYĆ
3.4.	GKSD_004	Urządzenie umożliwia dodatkową rozbudowę o warstwę typu CLOUD dedykowaną do długotrwałego przechowywania danych (tzw. Long Term Retention) – dane o określonej retencji (zgodnie z założoną polityka retencyjną), bez pośrednictwa dodatkowych urządzeń (typu GATEWAY) powinny zostać przemigrowane (w postaci zdeduplikowanej) na dodatkową warstwę (wymagane wsparcie dla dla AWS, Microsoft Azure, Google GCP). Wymagana enkrypcja danych przechowywanych na warstwie typu Cloud. Skalowanie w przypadku wykorzystywanej przestrzeni warstwy typu Cloud musi stanowić równoważność co najmniej dwukrotnej pojemności netto oferowanego urządzenia (bez uwzględnienia warstwy CLOUD).	MUSI BYĆ
3.5.	GKSD_005	Urządzenie umożliwia jednoczesny dostęp wszystkimi poniższymi protokołami: a) CIFS, NFS, b) zapewniającym deduplikację na źródle - wymagane wsparcie dla co najmniej Veeam Backup and Replication oraz NetWorker (rozwiązania w oparciu o FUSE filesystem wykluczone), c) VTL (po doposażeniu w porty FC).	MUSI BYĆ
3.6.	GKSD_006	Urządzenie osiąga zagregowaną wydajność (dla maksymalnej konfiguracji) protokołami CIFS, NFS: co najmniej 3 TB/h (dane podawane przez producenta) oraz co najmniej 7 TB/h z wykorzystaniem deduplikacji na źródle (dane podawane przez producenta).	MUSI BYĆ
3.7.	GKSD_007	Urządzenie pozwala na jednoczesną obsługę minimum 90 strumieni jednocześnie, w tym a) 30 dedykowanych do zapisu b) 30 dedykowanych do odczytu c) 30 dedykowanych do replikacji Wszystkie zapisywane strumienie podlegają globalnej deduplikacji przed zapisem na dysk (in-line) jak opisano w niniejszej specyfikacji.	MUSI BYĆ

Fundusze Europejskie na Rozwój Cyfrowy | Rzeczpospolita Polska | Dofinansowane przez Unię Europejską | Centrum Projektów Polska Cyfrowa

Lp.	ID	Nazwa wymagania	Wymagalność
3.8.	GKSD_008	Urządzenie deduplikuje dane in-line przed zapisem na nośnik dyskowy. Na wewnętrznych dyskach urządzenia nie mogą być zapisywane dane w oryginalnej postaci (niezdeduplikowanej) z jakiegokolwiek fragmentu strumienia danych przychodzącego do urządzenia, powyższe wymaganie nie będzie spełnione jeżeli deduplikacja in-line realizowana będzie przez zewnętrzną aplikację backup'ową. Wymaganie deduplikacji in-line dotyczy zapisu danych przez każdy z wymaganych intefejsów, w przypadku interfejsów: NFS, CIFS oraz VTL realizacja deduplikacji in-line nie może w żadnym stopniu zależeć od konkretnej aplikacji backu'owej, dane zapisywane poprzez interfejsy NFS CIFS bez użycia jakiejkolwiek aplikacji backup'owej również muszą być deduplikowane w sposób in-line.	MUSI BYĆ
3.9.	GKSD_009	Technologia deduplikacji wykorzystuje algorytm bazujący na zmiennym, dynamicznym bloku. Algorytm ten samoczynnie i automatycznie dopasowuje się do otrzymywanego strumienia danych co oznacza, że urządzenie dzieli otrzymany pojedynczy strumień danych na bloki o różnej długości, bez konieczności podejmowania czynności mających na celu ustalenie predefiniowanej długości bloków używanych do deduplikacji danych określonego typu.	MUSI BYĆ
3.10.	GKSD_010	Technologia deduplikacji wykorzystuje algorytm bazujący na zmiennym, dynamicznym bloku jednak o długości nie większej niż 12 kB Algorytm ten samoczynnie i automatycznie dopasowuje się do otrzymywanego strumienia danych co oznacza, że urządzenie dzieli otrzymany pojedynczy strumień danych na bloki o różnej długości, bez konieczności podejmowania czynności mających na celu ustalenie predefiniowanej długości bloków używanych do deduplikacji danych określonego typu. Deduplikacja zmiennym, dynamicznym blokiem oznacza, że wielkość każdego bloku (na jaki są dzielone dane pojedynczego strumienia backupowego) może być inna niż poprzedniego oraz jest indywidualnie ustalana przez algorytm deduplikacji zastosowany w urządzeniu, oferowane urządzenie nie może dzielić jakiegokolwiek pojedynczego strumienia danych backupowych na bloki o ustalonej, tej samej długości.	MUSI BYĆ
3.11.	GKSD_011	Urządzenie posiada obsługę mechanizmów globalnej deduplikacji dla danych otrzymywanych jednocześnie wszystkimi protokołami (CIFS, NFS, VTL, deduplikacja na źródle) przechowywanych w obrębie całej przestrzeni urządzenia co oznacza, że przechowywany na urządzeniu fragment danych nie może być ponownie zapisany bez względu na to, jakim protokołem zostanie ponownie otrzymany. Wszystkie emulowane jednocześnie w obrębie urządzenia biblioteki wirtualne (VTL) oraz udziały NFS/CIFS również powinny podlegać globalnej deduplikacji – blok danych otrzymany i zapisany w wirtualnej bibliotece „A", nie może zostać ponownie zapisany jeśli trafi do innej wirtualnej biblioteki „B" w obrębie tego samego urządzenia (to samo dotyczy udziałów NFS/CIFS). Przestrzeń składowania zdeduplikowanych danych musi być jedna dla wszystkich protokołów dostępowych, co oznacza zastosowanie pojedynczej bazy deduplikatów bez względu na ilość/rodzaj używanych jednocześnie protokołów dostępowych.	MUSI BYĆ
3.12.	GKSD_012	Przestrzeń składowania zdeduplikowanych danych jest jedna dla wszystkich protokołów dostępowych, co oznacza zastosowanie pojedynczej bazy deduplikatów bez względu na ilość/rodzaj używanych jednocześnie protokołów dostępowych.	MUSI BYĆ
3.13.	GKSD_013	Proces deduplikacji odbywa się in-line – w pamięci urządzenia, przed zapisem danych na nośnik dyskowy. Zapisowi na system dyskowy podlegają tylko unikalne bloki danych nie zapisane jeszcze na system dyskowy urządzenia. Dotyczy to każdego fragmentu przychodzących do urządzenia danych.	MUSI BYĆ
3.14.	GKSD_014	Urządzenie nie może w żadnej fazie korzystać (w całości lub częściowo) z bufora na składowanie danych w postaci oryginalnej (niezdeduplikowanej) w celu ich późniejszej deduplikacji (wymagana deduplikacja in-line).	MUSI BYĆ
3.15.	GKSD_015	Wszystkie unikalne bloki przed zapisaniem na dysk są kompresowane jedną z metod do wyboru: gz, lz.	MUSI BYĆ

Fundusze Europejskie na Rozwój Cyfrowy | Rzeczpospolita Polska | Dofinansowane przez Unię Europejską | Centrum Projektów Polska Cyfrowa

Lp.	ID	Nazwa wymagania	Wymagalność
3.16.	GKSD_016	Tryb zapisu zabezpieczanych danych nie umożliwia nadpisywania danych. Dane mogą być zapisywane jedynie w trybie append-only. Dane dla których wygasła retencja powinny zostać usunięte podczas procesu czyszczenia tzw. Cleaning. Wymaganie dotyczy wszystkich danych zapisanych na urządzeniu, a nie wybranych grup danych objętych działaniem blokad zabezpieczających przed usunięciem/modyfikacją danych.	MUSI BYĆ
3.17.	GKSD_017	Urządzenie wspiera (wymagane formalne wsparcie producenta urządzenia), co najmniej następujące aplikacje: Veeam, NetWorker.	MUSI BYĆ
3.18.	GKSD_018	W przypadku współpracy z każdą z poniższych aplikacji: a) Veeam Backup and Replication b) NetWorker urządzenie umożliwia deduplikację na źródle (w przypadku Veeam Backup and Replication: na poziomie - proxy Data Mover, w przypadku NetWorker na poziomie – Client i przesłanie nowych, nie znajdujących się jeszcze na urządzeniu bloków poprzez sieć LAN.) Deduplikacja w wyżej wymienionych przypadkach zapewnia aby do oferowanego urządzenia były transmitowane poprzez sieć LAN jedynie fragmenty danych nie znajdujące się dotychczas na urządzeniu. Urządzenie umożliwia deduplikację na źródle i przesłanie nowych, nie znajdujących się jeszcze na urządzeniu bloków poprzez sieć LAN. Deduplikacja w wyżej wymienionych przypadkach zapewnia aby z serwera do urządzenia były transmitowane poprzez sieć tylko fragmenty danych nie znajdujące się dotychczas na urządzeniu	MUSI BYĆ
3.19.	GKSD_019	W przypadku deduplikacji na źródle poprzez sieć IP (LAN oraz WAN), wymagana możliwość szyfrowania komunikacji kluczem minimum 256 bitów.	MUSI BYĆ
3.20.	GKSD_020	Oferowane urządzenie umożliwia uruchamianie maszyn wirtualnych VMware bezpośrednio z danych backupowych bez konieczności odtwarzania danych, funkcjonalność ta powinna być wspierana co najmniej przez Veeam Backup and Replication oraz NetWorker. Spełnienie wymagania nie może być ograniczone dla wybranych grup danych ze względu na miejsce składowania czy konkretną retencję.	MUSI BYĆ
3.21.	GKSD_021	Wymagane wsparcie dla backupów typu Virtual Synthetics co najmniej w przypadku aplikacji Veeam Backup and Replication oraz NetWorker.	MUSI BYĆ
3.22.	GKSD_022	Urządzenie nie może zmniejszać swojej wydajności w czasie przybywania kolejnych danych.	MUSI BYĆ
3.23.	GKSD_023	Oferowane urządzenie umożliwia bezpośrednią replikację danych do drugiego z oferowanych urządzeń oraz innych urządzeń takiego samego typu. Konfiguracja replikacji musi być możliwa w każdym z trybów: a) jeden do jednego b) wiele do jednego c) jeden do wielu d) kaskadowej (urządzenie A replikuje dane do urządzenia B, które te same dane replikuje do urządzenia C). Replikacja odbywa się w trybie asynchronicznym. Transmitowane mogą być tylko te fragmenty danych (bloki) które nie znajdują się na docelowym urządzeniu. Ewentualna licencja na replikację musi być dostarczona w ramach postępowania.	MUSI BYĆ
3.24.	GKSD_024	Urządzenie umożliwia wydzielenie określonych portów Ethernet dedykowanych do replikacji.	MUSI BYĆ
3.25.	GKSD_025	W przypadku wykorzystania portów Ethernet do replikacji urządzenie umożliwia przyjmowanie backupów, odtwarzanie danych, przyjmowanie strumienia replikacji, wysyłanie strumienia replikacji tymi samymi portami.	MUSI BYĆ

Lp.	ID	Nazwa wymagania	Wymagalność
3.26.	GKSD_026	Urządzenie działa poprawnie przy zapełnieniu danymi na poziomie co najmniej 90%. Dokumentacja urządzenia nie może wskazywać na ew. problemy, obostrzenia, które są efektem zapełnieniu urządzenia zabezpieczanymi danymi, na poziomie mniejszym niż 90%.	MUSI BYĆ
3.27.	GKSD_027	Urządzenie posiada możliwość ograniczenia pasma używanego do replikacji między dwoma urządzeniami.	MUSI BYĆ
3.28.	GKSD_028	Zdeduplikowane i skompresowane dane przechowywane w obrębie podsystemu dyskowego urządzenia są chronione za pomocą technologii RAID 6 lub równoważnej.	MUSI BYĆ
3.29.	GKSD_029	Urządzenie umożliwia realizację oraz przechowywanie SnapShot'ów, czyli umożliwiać zamrożenie obrazu danych (stanu backupów) w urządzeniu na określoną chwilę. Urządzenie umożliwia odtworzenie danych ze Snapshot'u. Odtworzenie danych ze Snapshot'u nie może wymagać konieczności nadpisania danych produkcyjnych jak również nie może oznaczać przerwy w normalnej pracy urządzenia (przyjmowania/odtwarzania backupów).	MUSI BYĆ
3.30.	GKSD_030	Urządzenie pozwala na realizację i przechowywanie minimum 300 Snapshotów jednocześnie w obrębie oferowanej przestrzeni, przy zachowaniu globalnej deduplikacji oraz standardowego trybu pracy urządzenia, umożliwiającego wykorzystanie wszystkich dostępnych funkcjonalności.	MUSI BYĆ
3.31.	GKSD_031	Urządzenie umożliwia podział na logiczne części. Dane znajdujące się w każdej logicznej części są między sobą deduplikowane (globalna deduplikacja między logicznymi częściami urządzenia).	MUSI BYĆ
3.32.	GKSD_032	Urządzenie posiada możliwość podziału na minimum 4 logiczne części pracujące równolegle.	MUSI BYĆ
3.33.	GKSD_033	Dla każdej z ww. logicznych części oferowanego urządzenia musi być możliwość zdefiniowania oddzielnego użytkownika zarządzającego daną logiczną częścią deduplikatora. Użytkownicy zarządzający logiczną częścią A muszą widzieć tylko i wyłącznie zasoby logicznej części A i nie mogą widzieć żadnych innych zasobów oferowanego urządzenia.	MUSI BYĆ
3.34.	GKSD_034	Możliwość zaprezentowania każdej z logicznych części oferowanego urządzenia, jako niezależnego urządzenia dostępnego za pośrednictwem: a) CIFS b) NFS c) zapewniającym deduplikację na źródle dla co najmniej: Veeam Backup and Replication oraz NetWorker d) VTL	MUSI BYĆ
3.35.	GKSD_035	Urządzenie umożliwia zdefiniowanie blokady skasowania danych (funkcjonalność WORM). Blokada skasowania danych chroni plik w zdefiniowanym czasie przed usunięciem pliku, modyfikacją pliku. Blokada skasowania danych działa w dwóch trybach (do wyboru przez administratora): a) Możliwość zdjęcia blokady przed upływem ważności danych b) Brak możliwości zdjęcia blokady przed upływem ważności danych (COMPLIANCE, wymagane wsparcie dla norm: SEC 17a-4(f) oraz ISO Standard 15489-1), wymagane oficjalne wsparcie aplikacji Veeam Backup and Replication oraz NetWorker. Licencje na blokadę skasowania/zmiany przechowywanych plików muszą być dostarczone wraz z urządzeniem. Wymagana możliwość automatycznego uruchamiania blokady (podczas zapisu) WORM dla danych zapisywanych na obszar objęty działaniem wspomnianej blokady, wymagana również możliwość używania blokady WORM dla obrazu danych uzyskanych poprzez użycie wymaganej funkcjonalności SnapShot. Zamawiający zastrzega możliwość prośby o dostarczenie ogólnodostępnej dokumentacji oferowanego produktu potwierdzającego spełnienie wymaganej funkcjonalności.	MUSI BYĆ

Lp.	ID	Nazwa wymagania	Wymagalność
3.36.	GKSD_036	Urządzenie weryfikuje ewentualne przekłamania (zmianę danych) na poziomie systemu plików. Wymaga się aby urządzenie weryfikowało sumy kontrolne dla wszystkich fragmentów zapisywanych danych, niezależnie od używanego interfejsu.	MUSI BYĆ
3.37.	GKSD_037	Urządzenie weryfikuje dane po zapisie (nie chodzi o ew. weryfikację danych indeksowych generowanych przez urządzenie ale o weryfikację wszystkich zabezpieczanych danych backup'owych w trybie „end-to-end"). Każda zapisana na dyskach porcja danych musi być odczytana i porównana z danymi otrzymanymi przez urządzenie. Powyższa weryfikacja powinna być realizowana w locie, czyli przed usunięciem z pamięci oryginalnych danych (otrzymanych z aplikacji backupowej), musi być realizowana w trybie ciągłym (a nie ad-hoc), wymagane parametry wydajnościowe urządzenia muszą uwzględniać tę funkcjonalność. Wymagane potwierdzenie opisanej funkcjonalności w oficjalnej dokumentacji producenta oferowanego urządzenia. Zamawiający zastrzega możliwość prośby o dostarczenie ogólnodostępnej dokumentacji oferowanego produktu potwierdzającego spełnienie wymaganej funkcjonalności)	MUSI BYĆ
3.38.	GKSD_038	Urządzenie posiada możliwość automatycznego usuwania przeterminowanych danych (bloki danych nie należące do backupów o aktualnej retencji) w procesie czyszczenia.	MUSI BYĆ
3.39.	GKSD_039	Proces usuwania przeterminowanych danych (czyszczenia) nie może uniemożliwiać pracy procesów backupu/odtwarzania danych (zapisu/odczytu danych z zewnątrz do systemu).	MUSI BYĆ
3.40.	GKSD_040	Urządzenie posiada możliwość zdefiniowania maksymalnego obciążenia urządzenia procesem usuwania przeterminowanych danych (poziomu obciążenia procesora). Zamawiający zastrzega możliwość prośby o dostarczenie ogólnodostępnej dokumentacji oferowanego produktu potwierdzającego spełnienie wymaganej funkcjonalności.	MUSI BYĆ
3.41.	GKSD_041	Urządzenie posiada możliwość zdefiniowania harmonogramu wg którego wykonywany jest proces usuwania przeterminowanych danych (czyszczenia), realizowany równolegle z procesami backup/restore/replication.	MUSI BYĆ
3.42.	GKSD_042	Standardowa częstotliwość usuwania przeterminowanych danych (czyszczenie) nie powinna być większa niż 1 raz na tydzień minimalizując czas w którym backupy/odtworzenia narażone są na spowolnienie (weryfikacja wymagania na podstawie dokumentacji typu DOBRE PRAKTYKI publikowanej przez producenta).	MUSI BYĆ
3.43.	GKSD_043	Urządzenie umożliwia systemowo (wbudowana funkcjonalność) realizację procesu pierwszego czyszczenia dopiero po przekroczeniu 75% zajętości oferowanej przestrzeni.	MUSI BYĆ
3.44.	GKSD_044	Urządzenie posiada możliwość zarządzania poprzez a) Interfejs graficzny dostępny z przeglądarki internetowej b) Poprzez linię komend (CLI) dostępną z poziomu ssh (secure shell)	MUSI BYĆ
3.45.	GKSD_045	Oprogramowanie do zarządzania rezyduje na oferowanym na urządzeniu deduplikacyjnym.	MUSI BYĆ
3.46.	GKSD_046	Urządzenie jest rozwiązaniem kompletnym, appliancem sprzętowym pochodzącym od jednego producenta. Zamawiający nie dopuszcza stosowania rozwiązań typu gateway. Oferowany typ urządzenia jest oficjalnie dostępny w ofercie producenta przed ukazaniem się niniejszego postępowania.	MUSI BYĆ
3.47.	GKSD_047	Serwer posiada min. 24 m-ce gwarancji producenta realizowanej w miejscu instalacji sprzętu z czasem reakcji następnego dnia roboczego od przyjęcia zgłoszenia. Możliwość zgłaszania awarii w trybie 24x7x365 (10 pkt. za udzielnie gwarancji 36 m-cy; 20 pkt. za udzielnie gwarancji 48 m-cy)	PUNKTOWANE

Lp.	ID	Nazwa wymagania	Wymagalność
3.48.	GKSD_048	Warunki usług gwarancyjnych: a) Zamawiający wymaga dostarczenia wraz z urządzeniem oświadczenia potwierdzającego, że w przypadku wystąpienia awarii dysku twardego w urządzeniu objętym aktywnym wparciem technicznym uszkodzony dysk twardy pozostaje u Zamawiającego. b) Firma serwisująca musi posiadać ISO 9001 na świadczenie usług serwisowych lub certyfikat równoważny. Zamawiający wymaga przedłożenia oświadczenia przedstawiciela producenta potwierdzającego posiadanie ISO 9001. c) Zamawiający wymaga dostarczenia wraz z urządzeniem oświadczenia przedstawiciela producenta potwierdzającego ważność uprawnień gwarancyjnych na terenie Polski.	MUSI BYĆ

4. [GKZA] WYMAGANIA TECHNICZNE W ZAKRESIE ZASILACZA AWARYJNEGO

W ramach tego podzadania ma być wykonana dostawa i instalacja 1 szt. zasilacza awaryjnego do serwerowni UGK. Zasilacz posiada następujące minimalne lub równoważne parametry:

Lp.	ID	Nazwa wymagania	Wymagalność
4.1.	GKZA_001	Zasilacz posiada obudowę o wysokość maksymalnie 4U, dedykowaną do zamontowania w szafie rack 19" wraz ze wspornikami do montażu w szafie.	MUSI BYĆ
4.2.	GKZA_002	Moc znamionowa: Min. 1980 W	MUSI BYĆ
4.3.	GKZA_003	Typ zasilacza: Line interactive	MUSI BYĆ
4.4.	GKZA_004	Gniazdo wejściowe IEC 320 C20	MUSI BYĆ
4.5.	GKZA_005	Gniazda wyjściowe z podtrzymaniem zasilania: a) IEC 320 C13 – min. 8 szt. b) IEC 320 C19 – min. 2 szt.	MUSI BYĆ
4.6.	GKZA_006	Czas podtrzymania przy obciążeniu 100%: Min. 9,5 minuty	MUSI BYĆ
4.7.	GKZA_007	Czas podtrzymania przy obciążeniu 50%: Min. 25 minut	MUSI BYĆ
4.8.	GKZA_008	Możliwość zwiększenia czasu podtrzymania przy obciążeniu 50% do min. 13 godzin poprzez dołączenie dodatkowych, zewnętrznych pakietów akumulatorowych.	MUSI BYĆ
4.9.	GKZA_009	Kształt napięcia wyjściowego: Sinusoidalny	MUSI BYĆ
4.10.	GKZA_010	Napięcie wejściowe: 230V	MUSI BYĆ
4.11.	GKZA_011	Porty komunikacji: USB, RJ-45 10/100 Base-T, RJ-45 Serial	MUSI BYĆ
4.12.	GKZA_012	Możliwość zarządzania zasilaczem przez sieć za pomocą przeglądarki	MUSI BYĆ
4.13.	GKZA_013	Możliwość rejestracji zdarzeń i powiadamiania o nich e-mailem	MUSI BYĆ
4.14.	GKZA_014	Możliwość monitorowania temperatury przy użyciu dołączonego czujnika temperatury	MUSI BYĆ
4.15.	GKZA_015	Wyświetlacz LCD pozwalający na odczyt następujących informacji: a) wartość napięcia wyjściowego, b) wartość napięcie wejściowego, c) częstotliwość wyjściowa, d) czas pracy na baterii, e) obciążenie, f) adres IP, g) numer seryjny zasilacza, h) numer produktu baterii, i) data instalacji baterii oraz sugerowana data jej wymiany.	MUSI BYĆ
4.16.	GKZA_016	Dołączone wyposażenie: a) Karta zdalnego zarządzania i monitorowania zasilacza przez sieć b) Kabel komunikacyjny USB c) Patchcord STP o długości 3m d) Oprogramowanie do zarządzania zasilaczem przez kabel USB oraz przez sieć e) Czujnik temperatury f) Płyta CD z oprogramowaniem	MUSI BYĆ
4.17.	GKZA_017	Gwarancja: Min. 24 miesiące	MUSI BYĆ

5. [GKZS] WYMAGANIA TECHNICZNE W ZAKRESIE ZARZĄDZALNEGO URZĄDZENIA SIECIOWEGO

W ramach tego podzadania ma być wykonana dostawa i instalacja 2 szt. zarządzalnych urządzeń sieciowych dla UGK. Zarządzalne urządzenie sieciowe posiada następujące minimalne lub równoważne parametry:

Lp.	ID	Nazwa wymagania	Wymagalność
5.1.	GKZS_001	W ramach postępowania wymagane jest dostarczenie elementów systemu niezbędnych do zbudowania bezpiecznej infrastruktury dostępowej. Poszczególne elementy systemu muszą zostać dostarczone w postaci komercyjnych platform sprzętowych lub programowych.	MUSI BYĆ
5.2.	GKZS_002	Parametry fizyczne platformy: a) Wymiary urządzenia umożliwiają na montaż w szafie rack 19", obudowa nie może być wyższa niż 1U. b) Zasilanie AC 230V. c) Maksymalny pobór mocy: 30 W.	MUSI BYĆ
5.3.	GKZS_003	Interfejsy sieciowe: Wymaganym jest aby przełącznik dysponował niezależnymi interfejsami sieciowymi (nie dopuszcza się portów typu combo) w ilości: a) Min. 24 porty GE RJ-45. b) Min. 4 porty 10 GE SFP+.	MUSI BYĆ
5.4.	GKZS_004	Zarządzanie: a) Wbudowany min. 1 port konsoli szeregowej do pełnego zarządzania. b) Zarządzanie przez: command line (w tym poprzez SSH) oraz poprzez graficzny interfejs z wykorzystaniem przeglądarki (HTTPS). c) Wsparcie dla SNMP w wersjach 1-3 d) Funkcja zarządzania poprzez dedykowany kontroler przełączników lub system zarządzania, pozwalający na automatyczne wykrywanie, centralne konfigurowanie oraz zarządzanie przełącznikami. e) Funkcja aktualizacji oprogramowania przez TFTP/FTP oraz za pomocą GUI. f) Konfiguracja w formie pliku tekstowego umożliwiającego edycję konfiguracji offline. g) Funkcja backupu konfiguracji z poziomu GUI jak również z CLI (TFTP/FTP). h) Funkcja definiowania administratorów lokalnie oraz wykorzystanie w tym celu serwerów Radius i TACACS+. i) Funkcja definiowania ról administratorów z możliwością określenia trybu dostępu (brak, tylko odczyt, odczyt oraz modyfikacja) do wybranych części konfiguracji. j) Automatycznie wykonywane rewizje konfiguracji.	MUSI BYĆ
5.5.	GKZS_005	Parametry wydajnościowe: a) Przepustowość urządzenia - min. 125 Gbps (pełna prędkość, tzw. wire-speed na wszystkich portach) oraz min. 190 Mpps. b) Tablica adresów MAC o pojemności co najmniej 32k wpisów. c) Opóźnienie wprowadzane przez przełącznik - poniżej 2 mikrosekund.	MUSI BYĆ

Fundusze Europejskie na Rozwój Cyfrowy | Rzeczpospolita Polska | Dofinansowane przez Unię Europejską | Centrum Projektów Polska Cyfrowa

Lp.	ID	Nazwa wymagania	Wymagalność
5.6.	GKZS_006	Wymagane funkcje: a) Funkcja automatycznej negocjacji prędkości i duplexu dla połączeń. b) Obsługa Jumbo Frames. c) Obsługa 802.1d (Spanning Tree), 802.1w (Rapid Spanning Tree), 802.1s (Multiple Spanning Tree). d) Agregacja portów zgodna ze standardem 802.3ad. e) Obsługa co najmniej 4000 VLAN'ów, zgodna ze standardem 802.1Q. f) Port-mirroring. g) Uwierzytelnianie 802.1x na poziomie portu. h) Uwierzytelnianie 802.1x w oparciu o adres MAC. i) W ramach 802.1x wsparcie dla dedykowanego VLAN'u dla gości (guest VLAN). j) W ramach 802.1x wsparcie dla urządzeń, które nie obsługują tego protokołu, na podstawie adresu MAC urządzenia. k) W ramach 802.1x wsparcie dla dynamicznego przypisywania VLAN.	MUSI BYĆ
5.7.	GKZS_007	Dodatkowe funkcje urządzenia przy integracji z systemem centralnego zarządzania / NAC: 1) Przełącznik wspiera tryb pracy, w którym jest zarządzany przez fizyczny element nadrzędny (przełącznik lub dedykowany kontroler) (tzw. port extender lub element leaf w architekturze spine-leaf). Zakres zarządzania przez element nadrzędny zawiera co najmniej: a) Centralne zarządzanie konfiguracją urządzenia b) Aktualizacja oprogramowania realizowana z systemu centralnego zarządzania c) Centralne zarządzanie sieciami VLAN. d) Blokowanie ruchu pomiędzy klientami w ramach jednego VLAN'u e) Rozpoznawanie urządzeń uzyskujących dostęp do sieci, zarówno stacji klienckich, jak i urządzeń typu drukarki, routery, przełączniki, itp.. f) Przenoszenie zidentyfikowanych urządzeń do właściwych stref. W przypadku wykrycia urządzenia niepasującego do zaakceptowanych schematów, urządzenie powinno przenieść go do strefy odizolowanej. g) Integrację z systemem kontroli dostępu. Urządzenie musi podejmować decyzje o dostępie na podstawie przynajmniej następujących czynników: nazwy hosta, nazwy użytkownika, typu urządzenia, typu systemu operacyjnego. h) Automatyczna detekcja i rekomendacje konfiguracji. i) Przesyłanie logów na zewnętrzny serwer syslog. j) Funkcja uruchomienia Captive Portalu w celu identyfikacji użytkowników. k) Obsługa białych i czarnych list adresów MAC. l) Wykrywanie aplikacji komunikujących się w sieci. 2) Możliwość redundantnego połączenia z elementami zarządzającymi. 3) W ramach postępowania koniecznym jest dostarczenie wszystkich licencji niezbędnych do uruchomienia na przełączniku ww. funkcji, polegających na integracji z systemem centralnego zarządzania lub NAC.	MUSI BYĆ
5.8.	GKZS_008	Funkcje urządzenia przy integracji z systemem centralnego zarządzania lub bezpieczeństwa: a) System realizuje funkcję Stateful Firewall pomiędzy sieciami VLAN realizowanymi na urządzeniu dostępowym. b) System zapewnia Routing statyczny i dynamiczny (co najmniej OSPF) oraz Policy Based Routing.	MUSI BYĆ
5.9.	GKZS_009	Gwarancja oraz wsparcie: System jest objęty serwisem gwarancyjnym producenta przez okres 24 miesięcy, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości. W ramach tego serwisu producent zapewnia również dostęp do aktualizacji oprogramowania oraz wsparcie techniczne w trybie 24x7. Oferent winien przedłożyć dokumenty: a) Oświadczanie Producenta lub Autoryzowanego Dystrybutora świadczącego wsparcie techniczne o gotowości świadczenia na rzecz Zamawiającego wymaganego serwisu (zawierające: adres strony internetowej serwisu i numer infolinii telefonicznej). b) Certyfikat ISO 9001 podmiotu serwisującego.	MUSI BYĆ

6. [GKOK] WYMAGANIA TECHNICZNE W ZAKRESIE OPROGRAMOWANIA DO WYKONYWANIA KOPII ZAPASOWYCH

W ramach tego podzadania ma być wykonana dostawa i instalacja subskrypcji na oprogramowanie do wykonywania kopii zapasowych. Oprogramowanie posiada następujące minimalne lub równoważne parametry:

Lp.	ID	Nazwa wymagania	Wymagalność
6.1.	GKOK_001	Oprogramowanie jest produktem przeznaczonym do obsługi środowisk DataCenter. Oferowany produkt znajduje 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 spełnia minimalne wymaganie: minimalna liczba referencji 150, minimalna ocena z referencji 4,5. Zamawiający wymaga dostarczenia wraz z oprogramowaniem wydruku potwierdzającego spełnienie wymogu.	MUSI BYĆ
6.2.	GKOK_002	Oprogramowanie współpracuje 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 są dostępne na wszystkich wspieranych platformach wirtualizacyjnych, chyba, że wyszczególniono inaczej.	MUSI BYĆ
6.3.	GKOK_003	Oprogramowanie zapewnia tworzenie kopii zapasowych z sieciowych urządzeń plikowych NAS opartych o SMB, CIFS i/lub NFS, obiektowych pamięci masowych kompatybilnych z Microsoft Azure, AWS S3 i urządzeń kompatybilnych z protokołem S3 oraz bezpośrednio z serwerów plikowych opartych o Windows i Linux.	MUSI BYĆ
6.4.	GKOK_004	Oprogramowanie jest niezależne sprzętowo i umożliwiać wykorzystanie dowolnej platformy serwerowej i dyskowej.	MUSI BYĆ
6.5.	GKOK_005	Oprogramowanie umożliwia tworzenie “samowystarczalnych” archiwów do odzyskania których nie wymagana jest osobna baza danych z metadanymi deduplikowanych bloków.	MUSI BYĆ
6.6.	GKOK_006	Oprogramowanie posiada mechanizmy deduplikacji i kompresji w celu zmniejszenia wielkości archiwów. Włączenie tych mechanizmów nie może skutkować utratą jakichkolwiek funkcjonalności wymienionych w tej specyfikacji.	MUSI BYĆ
6.7.	GKOK_007	Oprogramowanie przechowuje 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.	MUSI BYĆ
6.8.	GKOK_008	Oprogramowanie zapewnia 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.	MUSI BYĆ
6.9.	GKOK_009	Oprogramowanie pozwala 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 wspiera archiwizowanie tych danych do Microsoft Azure Archive Blob Storage oraz Amazon S3 Glacier.	MUSI BYĆ
6.10.	GKOK_010	Oprogramowanie wspiera niezmienność kopii zapasowych na potrzeby ochrony przed ransomware poprzez niedopuszczenie do usunięcia lub modyfikacji kopii zapasowej w zadanym okresie czasu.	MUSI BYĆ
6.11.	GKOK_011	Oprogramowanie nie instaluje żadnych stałych agentów wymagających wdrożenia czy upgradowania wewnątrz maszyny wirtualnej dla jakichkolwiek funkcjonalności backupu lub odtwarzania.	MUSI BYĆ
6.12.	GKOK_012	Oprogramowanie oferuje portal samoobsługowy, umożliwiający odtwarzanie użytkownikom wirtualnych maszyn, obiektów MS Exchange i baz danych MS SQL, Oracle oraz PostgreSQL (w tym odtwarzanie point-in-time).	MUSI BYĆ
6.13.	GKOK_013	Oprogramowanie zapewnia możliwość delegacji uprawnień do odtwarzania na portalu.	MUSI BYĆ

Lp.	ID	Nazwa wymagania	Wymagalność
6.14.	GKOK_014	Oprogramowanie posiada możliwość integracji z innymi systemami poprzez wbudowane RESTful API.	MUSI BYĆ
6.15.	GKOK_015	Oprogramowanie posiada wbudowane mechanizmy backupu konfiguracji w celu prostego odtworzenia systemu po całkowitej reinstalacji.	MUSI BYĆ
6.16.	GKOK_016	Oprogramowanie posiada wbudowane mechanizmy szyfrowania zarówno plików z backupami jak i transmisji sieciowej. Włączenie szyfrowania nie może skutkować utratą jakiejkolwiek funkcjonalności wymienionej w tej specyfikacji.	MUSI BYĆ
6.17.	GKOK_017	Oprogramowanie posiada mechanizmy chroniące przed utratą hasła szyfrowania.	MUSI BYĆ
6.18.	GKOK_018	Oprogramowanie posiada architekturę klient/serwer z możliwością instalacji wielu instancji konsoli administracyjnych.	MUSI BYĆ
6.19.	GKOK_019	Oprogramowanie posiada natywne mechanizmy uwierzytelniania wieloskładnikowego (MFA) w celu dostępu do konsoli administracyjnej.	MUSI BYĆ
6.20.	GKOK_020	Oprogramowanie wymaga autoryzacji dwóch administratorów backupu do wykonania krytycznych operacji (np. skasowanie backupu, dodanie kolejnego administratora).	MUSI BYĆ
6.21.	GKOK_021	Oprogramowanie posiada integracje z systemami zarządzania kluczami szyfrującymi (KMS).	MUSI BYĆ
6.22.	GKOK_022	Oprogramowanie posiada integracje z systemami typu SIEM.	MUSI BYĆ
6.23.	GKOK_023	Oprogramowanie wykorzystuje mechanizmy Change Block Tracking na wszystkich wspieranych platformach wirtualizacyjnych. Mechanizmy są certyfikowane przez dostawcę platformy wirtualizacyjnej.	MUSI BYĆ
6.24.	GKOK_024	Oprogramowanie wykorzystuje mechanizmy śledzenia zmienionych plików przy zabezpieczaniu udziałów plikowych.	MUSI BYĆ
6.25.	GKOK_025	Oprogramowanie oferuje możliwość sterowania obciążeniem storage'u produkcyjnego tak aby nie były przekraczane skonfigurowane przez administratora backupu poziomy latencji. Funkcjonalność ta jest dostępna na wszystkich wspieranych platformach wirtualizacyjnych z dokładnością do pojedynczego datastore'u.	MUSI BYĆ
6.26.	GKOK_026	Oprogramowanie zapewnia tworzenie kopii zapasowych z bezpośrednim wykorzystaniem snapshotów macierzowych. Zapewnia też odtwarzanie maszyn wirtualnych z takich snapshotów. Proces wykonania kopii zapasowej nie może wymagać użycia jakichkolwiek hostów tymczasowych. Opisana funkcjonalność powinna działać w środowisku VMware.	MUSI BYĆ
6.27.	GKOK_027	Oprogramowanie posiada wsparcie dla VMware vSAN potwierdzone odpowiednią certyfikacją VMware.	MUSI BYĆ
6.28.	GKOK_028	Oprogramowanie wspiera kopiowanie backupów oraz zasobów plikowych na taśmy (LTO oraz IBM 3592).	MUSI BYĆ
6.29.	GKOK_029	Oprogramowanie ma możliwość tworzenia retencji GFS (Grandfather-Father-Son).	MUSI BYĆ
6.30.	GKOK_030	Oprogramowanie wspiera bezpośrednią integrację z urządzeniami deduplikacyjnymi. Minimalnie wsparcie wymagane dla Dell DataDomain, HPE StoreOnce, ExaGrid, Fujitsu CS800, Quantum DXi oraz Infinidat InfiniGuard.	MUSI BYĆ
6.31.	GKOK_031	Oprogramowanie wspiera 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.	MUSI BYĆ
6.32.	GKOK_032	Oprogramowanie posiada możliwość kopiowania backupów oraz replikacji wirtualnych maszyn z wykorzystaniem wbudowanej akceleracji WAN.	MUSI BYĆ
6.33.	GKOK_033	Oprogramowanie posiada możliwość replikacji asynchronicznej włączonych wirtualnych maszyn bezpośrednio z infrastruktury VMware vSphere pomiędzy hostami ESXi oraz pomiędzy hostami Hyper-V. Dodatkowo oprogramowanie posiada możliwość użycia plików kopii zapasowych jako źródła replikacji.	MUSI BYĆ

Lp.	ID	Nazwa wymagania	Wymagalność
6.34.	GKOK_034	Oprogramowanie posiada możliwość replikacji ciągłej, opartej o VMware VAIO, włączonych wirtualnych maszyn bezpośrednio z infrastruktury VMware vSphere. Dla replikacji ciągłej jest możliwość zdefiniowania dziennika pozwalającego na odzyskanie danych z dowolnego punku w ramach ustalonego parametru RPO.	MUSI BYĆ
6.35.	GKOK_035	Oprogramowanie umożliwia przechowywanie punktów przywracania dla replik.	MUSI BYĆ
6.36.	GKOK_036	Oprogramowanie umożliwia wykorzystanie istniejących w infrastrukturze wirtualnych maszyn jako źródła do dalszej replikacji (replica seeding).	MUSI BYĆ
6.37.	GKOK_037	Oprogramowanie wykorzystuje wszystkie oferowane przez hypervisor tryby transportu (sieć, hot-add, LAN Free-SAN).	MUSI BYĆ
6.38.	GKOK_038	Oprogramowanie umożliwia 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. Dodatkowo dla środowiska vSphere, Hyper-V i Nutanix AHV powyższa funkcjonalność umożliwia uruchomianie backupu z innych platform (inne wirtualizatory, maszyny fizyczne oraz chmura publiczna).	MUSI BYĆ
6.39.	GKOK_040	Oprogramowanie pozwala na migrację on-line tak uruchomionych maszyn na storage produkcyjny. Migracja odbywa się mechanizmami wbudowanymi w hypervisor. Jeżeli licencja na hypervisor nie posiada takich funkcjonalności - oprogramowanie realizuje taką migrację swoimi mechanizmami.	MUSI BYĆ
6.40.	GKOK_041	Oprogramowanie pozwala na zaprezentowanie pojedynczego dysku bezpośrednio z kopii zapasowej do wybranej działającej maszyny wirtualnej vSphere.	MUSI BYĆ
6.41.	GKOK_042	Oprogramowanie pozwala na uruchomienie zasobów plikowych SMB oraz baz danych MS SQL, Oracle i PostgreSQL bezpośrednio ze skompresowanego pliku backupu. Dodatkowo wspierana jest migracja on-line tak uruchomionych zasobów na środowisko produkcyjne.	MUSI BYĆ
6.42.	GKOK_043	Oprogramowanie umożliwia pełne odtworzenie wirtualnej maszyny, plików konfiguracji i dysków.	MUSI BYĆ
6.43.	GKOK_044	Oprogramowanie umożliwia pełne odtworzenie wirtualnej maszyny bezpośrednio do Microsoft Azure, Microsoft Azure Stack, Amazon EC2 oraz Google Cloud Platform.	MUSI BYĆ
6.44.	GKOK_045	Oprogramowanie umożliwia odtworzenie plików/folderów lub ich uprawnień na maszynę operatora, lub na serwer produkcyjny bez potrzeby użycia agenta instalowanego wewnątrz wirtualnej maszyny. Funkcjonalność ta nie jest ograniczona wielkością i liczbą przywracanych plików.	MUSI BYĆ
6.45.	GKOK_046	Oprogramowanie posiada możliwość odtworzenia plików bezpośrednio do maszyny wirtualnej poprzez sieć przy pomocy natywnego API dla platformy VMware i PowerShell Direct dla platformy Hyper-V.	MUSI BYĆ
6.46.	GKOK_047	Oprogramowanie wspiera odtwarzanie pojedynczych plików z systemów Windows, Linux, BSD, Solaris, Mac, Novell.	MUSI BYĆ
6.47.	GKOK_048	Oprogramowanie wspiera przywracanie plików z partycji Linux LVM.	MUSI BYĆ
6.48.	GKOK_049	Oprogramowanie umożliwia szybkie, granularne odtwarzanie obiektów aplikacji bez użycia jakiegokolwiek agenta zainstalowanego wewnątrz maszyny wirtualnej.	MUSI BYĆ
6.49.	GKOK_050	Oprogramowanie wspiera 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 pozwala na odtworzenie haseł.	MUSI BYĆ
6.50.	GKOK_051	Oprogramowanie wspiera granularne odtwarzanie Microsoft Exchange 2013SP1 i nowszych (dowolny obiekt w tym obiekty w folderze "Permanently Deleted Objects"). Odtwarzanie jest możliwe bezpośrednio do środowiska produkcyjnego.	MUSI BYĆ
6.51.	GKOK_052	Oprogramowanie wspiera granularne odtwarzanie Microsoft SQL 2008 i nowszych. Odtwarzanie jest możliwe bezpośrednio do środowiska produkcyjnego dla odzysku point-in-time, całych baz lub pojedynczych tabeli, widoków oraz procedur.	MUSI BYĆ

Lp.	ID	Nazwa wymagania	Wymagalność
6.52.	GKOK_053	Oprogramowanie wspiera granularne odtwarzanie Microsoft Sharepoint 2013 i nowszych. Odtwarzanie jest możliwe bezpośrednio do środowiska produkcyjnego dla odzysku całych witryn, bibliotek oraz pojedynczych dokumentów wraz z historią ich wersji.	MUSI BYĆ
6.53.	GKOK_054	Oprogramowanie wspiera granularne odtwarzanie baz danych Oracle z opcją odtwarzanie point-in-time wraz z włączonym Oracle DataGuard. Funkcjonalność ta jest dostępna dla baz uruchomionych w środowiskach Windows oraz Linux.	MUSI BYĆ
6.54.	GKOK_055	Oprogramowanie wspiera granularne odtwarzanie baz danych PostgreSQL z opcją odtwarzanie point-in-time. Funkcjonalność ta jest dostępna dla baz uruchomionych w środowiskach Linux.	MUSI BYĆ
6.55.	GKOK_056	Oprogramowanie wspiera granularne odtwarzanie baz danych SAP HANA do oryginalnej lub innej lokalizacji.	MUSI BYĆ
6.56.	GKOK_057	Oprogramowanie posiada natywną integrację dla backupów wykonywanych poprzez Oracle RMAN.	MUSI BYĆ
6.57.	GKOK_058	Oprogramowanie posiada natywną integrację dla backupów wykonywanych poprzez SAP HANA, SAP Oracle.	MUSI BYĆ
6.58.	GKOK_059	Oprogramowanie posiada natywną integrację dla backupów wykonywanych poprzez MS SQL VDI.	MUSI BYĆ
6.59.	GKOK_060	Oprogramowanie posiada natywną integrację dla backupów wykonywanych poprzez IBM Db2.	MUSI BYĆ
6.60.	GKOK_061	Oprogramowanie wspiera specyficzne metody odtwarzania w tym "reverse CBT" oraz odtwarzanie z wykorzystaniem sieci SAN.	MUSI BYĆ
6.61.	GKOK_062	Oprogramowanie daje możliwość stworzenia laboratorium (izolowane środowisko) dla vSphere i Hyper-V używając wirtualnych maszyn uruchamianych bezpośrednio z plików backupu. Powyższa funkcjonalność umożliwia uruchomianie backupu z innych platform (inne wirtualizatory, maszyny fizyczne oraz chmura publiczna).	MUSI BYĆ
6.62.	GKOK_063	Dla VMware'a oprogramowanie pozwala na uruchomienie takiego środowiska dla replik maszyn wirtualnych oraz bezpośrednio ze snapshot'ów macierzowych stworzonych na wspieranych urządzeniach.	MUSI BYĆ
6.63.	GKOK_064	Oprogramowanie umożliwia 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.	MUSI BYĆ
6.64.	GKOK_065	Oprogramowanie umożliwia 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.	MUSI BYĆ
6.65.	GKOK_066	Oprogramowanie analizuje indeksy systemów plików zabezpieczanych maszyn w poszukiwaniu rozszerzeń, notatek żądania okupu oraz innych oznak obecności ransomware/malware.	MUSI BYĆ
6.66.	GKOK_067	Oprogramowanie posiada możliwość skanowania plików backupu przy pomocy znanych sygnatur złośliwego oprogramowania.	MUSI BYĆ
6.67.	GKOK_068	Oprogramowanie, bazując na wyuczonym modelu maszynowym (machine learning) pozwala w locie wykrywać oznaki złośliwego oprogramowania (malware, ransomware) oraz cyberataków.	MUSI BYĆ
6.68.	GKOK_069	Oprogramowanie umożliwia dwuetapowe, automatyczne, odtwarzanie maszyn wirtualnych z możliwością wstrzyknięcia dowolnego skryptu przed odtworzeniem danych do środowiska produkcyjnego.	MUSI BYĆ
6.69.	GKOK_070	Oprogramowanie posiada możliwość wykonywania kopii zapasowej systemu Windows oraz Linux wykorzystując agenta znajdującego się wewnątrz systemu operacyjnego.	MUSI BYĆ

Lp.	ID	Nazwa wymagania	Wymagalność
6.70.	GKOK_071	Oprogramowanie wspiera systemy operacyjne Windows w wersjach klienckich oraz serwerowych.	MUSI BYĆ
6.71.	GKOK_072	Oprogramowanie wspiera co najmniej następujące dystrybucje systemów Linux: Debian, Ubuntu, RHEL, CentOS, Oracle Linux, SLES, Fedora, openSUSE.	MUSI BYĆ
6.72.	GKOK_073	Oprogramowanie wspiera system operacyjny macOS.	MUSI BYĆ
6.73.	GKOK_074	Oprogramowanie wspiera odtwarzanie pojedynczych plików z systemów Windows, Linux, MacOS, Unix.	MUSI BYĆ
6.74.	GKOK_075	Oprogramowanie posiada możliwość instalacji oraz zarządzania wykorzystując tryb niezależny (per agent) jak również zcentralizowany (poprzez centralną konsolę zarządzającą).	MUSI BYĆ
6.75.	GKOK_076	Oprogramowanie wspiera systemy oparte o Microsoft Failover Cluster.	MUSI BYĆ
6.76.	GKOK_077	Oprogramowanie wspiera zabezpieczanie do oraz odzyskiwanie z urządzeń blokowych pozwalając na odzysk całej maszyny (tzw. bare metal recovery) wybranych wolumenów, oraz wybranych plików i folderów.	MUSI BYĆ
6.77.	GKOK_078	Oprogramowanie wspiera backup podłączonych dysków USB.	MUSI BYĆ
6.78.	GKOK_079	Kopia zapasowa całej maszyny oraz pojedynczych wolumenów jest wykonywana na poziomie blokowym.	MUSI BYĆ
6.79.	GKOK_080	Oprogramowanie pozwala 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).	MUSI BYĆ
6.80.	GKOK_081	Oprogramowanie wspiera deduplikację oraz kompresję na źródle. Dane wysyłane na repozytorium są już odpowiednio przetworzone.	MUSI BYĆ
6.81.	GKOK_082	Oprogramowanie wspiera kontrolę pasma sieciowego.	MUSI BYĆ
6.82.	GKOK_083	Oprogramowanie wspiera ograniczenie wykonywania backupów dla konkretnych sieci bezprzewodowych.	MUSI BYĆ
6.83.	GKOK_084	Oprogramowanie wspiera ograniczenia wykonywania backupów dla połączeń VPN.	MUSI BYĆ
6.84.	GKOK_085	Oprogramowanie wspiera śledzenie zmienionych bloków podczas wykonywania kopii zapasowych.	MUSI BYĆ
6.85.	GKOK_086	Oprogramowanie wspiera technologię BitLocker.	MUSI BYĆ
6.86.	GKOK_087	Oprogramowanie wspiera uruchamianie z nośnika odtwarzania.	MUSI BYĆ
6.87.	GKOK_088	Oprogramowanie wspiera 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.	MUSI BYĆ
6.88.	GKOK_089	Oprogramowanie wspiera odzysk do konkretnego punktu w czasie (point-in-time) dla wspieranych systemów bazodanowych.	MUSI BYĆ
6.89.	GKOK_090	Oprogramowanie umożliwia natychmiastowe publikowanie baz MS SQL, Oracle I PostgreSQL poprzez bezpośrednie uruchomienie ich z pliku backupu.	MUSI BYĆ
6.90.	GKOK_091	Oprogramowanie wspiera odzysk obrazów kopii zapasowych bezpośrednio do vSphere, Hyper-V, Nutanix AHV, Microsoft Azure, Microsoft Azure Stack, Amazon EC2 oraz Google Cloud Platform.	MUSI BYĆ
6.91.	GKOK_092	Oprogramowanie wspiera szyfrowanie.	MUSI BYĆ

Lp.	ID	Nazwa wymagania	Wymagalność
6.92.	GKOK_093	Oprogramowanie wspiera możliwość wykonywania kopii zapasowych stacji klienckich, lokalnie do repozytorium tymczasowego (cache) gdy połączenie sieciowe do głównego repozytorium kopii zapasowych jest niedostępne.	MUSI BYĆ
6.93.	GKOK_094	Oprogramowanie posiada funkcjonalność automatycznego zmniejszenia szybkości przetwarzania danych, aby nie dopuścić do obniżenia wydajności systemu zabezpieczanego.	MUSI BYĆ
6.94.	GKOK_095	Oprogramowanie posiada ochronę przed ransomware poprzez automatyczne odmontowanie nośnika po wykonanym backupie stacji klienckiej.	MUSI BYĆ
6.95.	GKOK_096	Oprogramowanie wspiera tworzenie wielu zadań backupowych.	MUSI BYĆ
6.96.	GKOK_097	Licencja oparta na subskrypcji na okres do 01 maja 2026.	MUSI BYĆ
6.97.	GKOK_098	Licencja oparta na subskrypcji dla 7 szt. wirtualnych maszyn, 3 szt. serwerów fizycznych oraz 25 stacji roboczych. Wsparcie techniczne udzielane w trybie 24/7.	MUSI BYĆ