Załącznik nr 11 do SWZ

**OPIS PRZEDMIOTU ZAMÓWIENIA**

**I. Macierz – 1 szt.**

Przedmiotem zamówienia jest dostawa, instalacja oraz konfiguracja macierzy blokowej do zadań produkcyjnych.

Wymagania:

1. Obudowa do montażu w szafie rack 19” za pomocą dostarczonych dedykowanych elementów. Oferowana macierz nie może przekroczyć rozmiaru 2U. Oferowana obudowa musi umożliwiać instalację min 25 dysków.

2. Macierz wyposażona w minimum 2 kontrolery pracujące w trybie active-active. Akceptowalna architektura to symmetric active-active, to znaczy pracę kontrolerów w trybie zapewniającym dostęp do wolumenów logicznych (LUN) utworzonych w macierzy, z wykorzystaniem wszystkich dostępnych ścieżek (path) i portów kontrolerów bez wymuszania preferowanej ścieżki dostępu oraz z zapewnieniem automatycznego równoważenia obciążenia (load balancing). Kontrolery nie mogą pracować w trybie active-passive.

3. Oferowane urządzenie musi być przystosowane do zasilania z sieci AC oraz wyposażone w kable zasilające PDU. Macierz musi być wyposażona w zdublowany, redundantny system zasilania, umożliwiający prawidłową, nieprzerwaną pracę urządzenia w przypadku awarii dowolnego pojedynczego źródła zasilania.

4. Surowa przestrzeń dyskowa (RAW) zbudowana tylko i wyłącznie za pomocą dysków SSD SAS musi wynosić min. 38 TB. Przestrzeń użytkowa musi być zbudowana z RAID 6 z 1 dyskiem hot-spare lub przestrzenią hot-spare równą pojemności 1 dysku. Ze względów wydajnościowych oraz niezawodnościowych rozmiar pojedynczego dysku nie może być większy niż 4 TB, co przełoży się na większą liczbę dysków.

5. Dyski muszą być wyposażone w podwójne interfejsy. Niedopuszczalne są dyski SSD zbudowane w oparciu o chipset QLC ze względu na skróconą żywotność.

6. Możliwość definiowania przez administratora dysków SPARE lub odpowiedniej zapasowej przestrzeni dyskowej.

7. Rozbudowa oferowanej macierzy, do co najmniej 80 szt dysków SSD SAS, bez wymiany kontrolerów macierzowych oraz bez rozbudowy o dodatkowe kontrolery, tylko poprzez dodawanie półek i dysków SSD SAS. Macierz nie może obsługiwać dysków HDD.

8. Co najmniej 64GB pamięci cache na całą macierz (dwa kontrolery). Zamawiający nie dopuszcza możliwości zastosowania dysków SSD/NVMe lub kart pamięci FLASH jako rozszerzenia pamięci cache. Pamięć cache musi być zabezpieczona przed utratą danych w przypadku awarii zasilania poprzez funkcję zapisu zawartości pamięci cache na nieulotną pamięć.

9. Razem kontrolery muszą udostępnić minimum 4 porty optyczne 10Gb Eth, 8 portów miedzianych 1Gb Eth oraz 8 portów 25G SFP28 Eth. Wymagana możliwość rozbudowy o dodatkowe 8 portów 10Gb lub 25G Eth bez konieczności wymiany lub zakupu nowych kontrolerów i klastrowania z kontrolerami oferowanymi w tym postępowaniu. Wszystkie moduły muszą posiadać wkładki optyczne SFP+ i SFP28.

10. Macierz musi posiadać wbudowane min 4 porty SAS 12Gb/s do podłączenia półek dyskowych.

11. Wymagane wsparcie dla FC, iSCSI.

12. Kontrolery wyposażone w funkcjonalność konfiguracji poziomu RAID 6 lub równoważnego tolerującego jednoczesną awarię 2 dysków bez utraty danych.

13. Wymagana funkcjonalność tworzenia i prezentacji dysków logicznych (LUN) o pojemności większej niż zajmowana fizyczna przestrzeń dyskowych (ang. ThinProvisioning). Wymagana funkcjonalność zwrotu skasowanej przestrzeni dyskowej do puli zasobów wspólnych (ang. Space Reclamation). Macierz musi wspierać nie mniej niż 1024 LUNów. Wymagana możliwość tworzenia grup wolumenów. Max liczba LUNów w grupie wolumenów nie może być mniejsza niż 100. Wymagane dostarczenie w/w funkcjonalności na zainstalowaną przestrzeń dyskową.

14. Zarządzanie macierzą (wszystkimi kontrolerami) z poziomu pojedynczego interfejsu graficznego. Wymagane jest stałe monitorowanie stanu macierzy w tym monitorowanie wydajności obiektów takich jak:

a. cała macierz

b. kontrolery

c. porty front-end

d. dyski

e. LUNy

f. hosty

Pod kątem parametrów takich jak:

a. operacje wejścia/wyjścia IOPS

b. przepustowość (KB/s lub MB/s)

c. czas odpowiedzi (latency)

Wymagana możliwość monitorowania stanu żywotności dysków SSD SAS. Wymagana możliwość dostępu do historycznych danych wydajnościowych z poziomu GUI macierzy do co najmniej 2 lat wstecz lub jako równoważne dostarczenie fizycznego serwera z oprogramowaniem umożliwiającym zbieranie i przeglądanie danych historycznych.

Wymagana możliwość konfigurowania zasobów macierzy.

Jeżeli do obsługi powyższej funkcjonalności wymagane są dodatkowe licencje, ich dostarczenie jest wymagane na tym etapie postępowania.

15. Tworzenie na żądanie tzw. migawkowej kopii danych (ang. snapshot) w ramach macierzy do wykorzystania w celu np. wykonywania kopii zapasowych. Snapshoty muszą być wykonywanie w technologii ROW (Redirect On Write). Macierz musi obsługiwać min 2000 snapshotów. Wymagane wsparcie dla snapshotów kaskadowych.nWymagana możliwość tworzenia harmonogramu wykonywania snapshotów oraz zabezpieczenia migawek przed modyfikacją lub usunięciem pod kątem szybkiego przywrócenia danych w przypadku ataku ransomware. Dostarczenie powyższych funkcjonalności jest wymagane na tym etapie postępowania na całą przestrzeń dyskową i na maksymalną liczbę snapshotów obsługiwanych przez oferowany model macierzy.

16. Tworzenie na żądanie kopii danych typu klon w ramach macierzy za pomocą wewnętrznych kontrolerów macierzowych. Funkcjonalność ta musi umożliwiać synchronizację danych z wolumenu źródłowego na docelowy oraz resynchronizację danych z wolumenu docelowego na źródłowy. Dostarczenie tej funkcjonalności jest wymagane na tym etapie postępowania.

17. Możliwość zdalnej replikacji danych typu on-line (bez przerywania prezentacji wolumenów dyskowych) do macierzy tej samej rodziny w trybie asynchronicznym oraz synchronicznym przy wykorzystaniu portów FC lub IP. Funkcjonalność ta nie może wpływać na obciążenie serwerów podłączonych do macierzy. Dostarczenie tej funkcjonalności nie jest wymagane na tym etapie postępowania.

18. Wsparcie dla technologii klastrowania macierzy dyskowych (ang. Storage Metro Cluster). Macierz musi dostarczać funkcjonalność klastra klasy "wysokiej dostępności" tj. zapewnienia wysokiej dostępności zasobów dyskowych macierzy dla podłączonych platform oprogramowania i sprzętowych z wykorzystaniem synchronicznej replikacji danych po protokole FC lub IP pomiędzy 2 macierzami. Pod użytym pojęciem "wysoka dostępność zasobów dyskowych" należy rozumieć zapewnienie bezprzerwowego działania środowiska (aplikacja/system operacyjny/serwer) podłączonego do macierzy (macierz preferowana) w przypadku wystąpienia awarii logicznego połączenia z tą macierzą bądź awarii samej macierzy powodujących dla danego środowiska brak dostępu do zasobów macierzy preferowanej. Funkcjonalność klastra "wysokiej dostępności" pozwala na automatyczne przełączanie obsługi środowisk produkcyjnych z macierzy preferowanej na niepreferowaną w przypadku awarii macierzy preferowanej (tzw. automated failover). Wymagany jest również automatyczny failover z macierzy niepreferowanej na preferowaną. Dopuszczalne jest zastosowanie tzw arbitra (serwer quorum). Dostarczenie tej funkcjonalności nie jest wymagane na tym etapie postępowania.

19. Macierz musi posiadać możliwość zapewnienia ciągłości biznesu na oczekiwanym poziomie usług (QoS) poprzez definicję polityk QoS w oparciu o maksymalne progi wydajności IOPS i MB/s. Musi istnieć możliwość określenia polityk QoS na poziomie wolumenów. Dostarczenie tej funkcjonalności jest wymagane na tym etapie postępowania.

20. Macierz musi oferować wsparcie dla zachowania integralności danych na całej ścieżce transferu (ang. End-to-End) zgodnego ze standardem/specyfikacją T10 PI.

21. Wsparcie, dla co najmniej Microsoft Server Windows 2016/2019/2022, VMware 6.x/7.x, Linux RedHat 7.x/8.x, CentOS 7.x/8.x

22. Wymagane uaktualnianie firmware-u kontrolerów macierzy bez przerywania dostępu do danych.

23. Macierz przystosowana do napraw w miejscu zainstalowania oraz wymiany elementów bez konieczności jej wyłączania.

24. Macierz musi umożliwiać zdalne zarządzanie.

25. Urządzenie musi być fabrycznie nowe, wyprodukowane nie wcześniej niż 6 miesięcy przed datą dostarczenia do Zamawiającego i musi być objęte serwisem producenta lub autoryzowanego partnera serwisowego na terenie RP.

26. Urządzenie musi być zakupione w oficjalnym kanale dystrybucyjnym producenta. Na wezwanie Zamawiającego należy dostarczyć oświadczenie producenta oferowanej macierzy, potwierdzające pochodzenie urządzenia z oficjalnego kanału dystrybucyjnego producenta.

27. Wymagana gwarancja na 36 miesięcy w trybie 9x5 NBD.

28. W przypadku awarii, uszkodzone dyski pozostają u Zamawiającego tj. Zamawiający wymaga dostarczenia disk retention.

29. Na wezwanie Zamawiającego należy dostarczyć oświadczenie producenta z potwierdzeniem zaoferowanego poziomu gwarancji.

30. Zakres prac wdrożeniowych:

a. Opracowanie planu wdrożenia.

b. Instalacja macierzy wraz z wymaganymi licencjami i oprogramowaniem.

c. Konfiguracja macierzy zgodnie z wymaganiami zamawiającego.

d. Integracja z istniejącymi systemami IT zamawiającego.

e. Przeprowadzenie testów funkcjonalnych i wydajnościowych wymaganych przez Zamawiającego potwierdzających zadeklarowane funkcjonalności. Wynik negatywny jakiejkolwiek funkcjonalności lub testu pozwala Zamawiającemu odrzucić proponowaną ofertę i odstąpić od umowy bez podania przyczyny.

f. Weryfikacja poprawności działania macierzy.

**II. Deduplikator – 1 szt.**

Przedmiotem zamówienia jest dostawa, instalacja oraz konfiguracja deduplikatora do zadań backupowych.

Wymagania:

1. Obudowa do montażu w szafie rack 19” za pomocą dostarczonych dedykowanych elementów. Oferowany deduplikator nie może przekroczyć rozmiaru 2U. Oferowana obudowa musi umożliwiać instalację min 12 dysków.

2. Deduplikator musi być wyposażony w minimum 2 kontrolery pracujące w trybie active-passive lub active-active. Deduplikator nie może posiadać pojedynczego punktu awarii, który powodowałby brak dostępu do danych. W przypadku awarii kontrolera wszystkie procesy musi przejąć drugi kontroler.

3. Oferowany model deduplikatora musi osiągać w maksymalnej konfiguracji zagregowaną wydajność backupu co najmniej 5 TB/h (dane podawane przez producenta). Dodatkowo wymagana zagregowana wydajność backupu przy zastosowaniu deduplikacji na źródle co najmniej 8 TB/h (dane podawane przez producenta).

4. Surowa przestrzeń dyskowa (RAW) stworzona w oparciu o dyski NL SAS musi wynosić min. 64 TB. Dyski muszą być skonfigurowane w RAID 6 z min. 1 dyskiem hot-spare lub przestrzenią hot-spare równą pojemności min. 1 dysku. Dodatkowo wymagane jest zastosowanie co najmniej 4 dysków SSD SAS o łącznej pojemności RAW min 3,84 TB jako cache pod zapis backupu.

5. Dane przechowywane w obrębie podsystemu dyskowego urządzenia muszą być chronione za pomocą technologii RAID 6 lub równoważnej tolerującej jednoczesną awarię 2 dysków bez utraty danych. Urządzenie musi umożliwiać bezpieczne usuwanie danych zgodnie ze standardem DoD 5220.22-M poprzez mechanizm nadpisywania danych.

6. Wymagana możliwość rozbudowy przestrzeni użytkowej poprzez instalację dysków i półek dyskowych oraz dodanie licencji (jeśli będzie wymagana) do min 250 TB.

7. Co najmniej 256GB pamięci cache na cały deduplikator (dwa kontrolery). Pamięć cache musi być zabezpieczona przed utratą danych w przypadku awarii zasilania.

8. Urządzenie musi posiadać minimum:

a. 8 portów RJ45 Ethernet 1 Gb/s, 4 porty SFP+ Ethernet 10 Gb/s oraz 8 portów SFP28 Ethernet 25Gb/s z możliwością obsługi każdym portem Ethernet protokołów CIFS, NFS.

b. Wszystkie porty SFP+ oraz SFP28 wyposażone we wkładki optyczne MM.

9. Wymagana możliwość agregowania portów (bond port).

10. Wymagane wsparcie dla FC, iSCSI, NFS, CIFS.

11. Zarządzanie deduplikatorem (wszystkimi kontrolerami) z poziomu pojedynczego interfejsu graficznego. Wymagane jest stałe monitorowanie stanu deduplikatora w tym monitorowanie wydajności obiektów takich jak:

a. cały deduplikator

b. kontrolery

c. CPU

d. porty front-end

e. porty logiczne

f. dyski

g. file systemy

12. Wymagane jest stałe monitorowanie stanu deduplikatora pod kątem parametrów takich jak:

a. operacje wejścia/wyjścia IOPS

b. przepustowość (KB/s lub MB/s)

c. czas odpowiedzi (latency)

d. średnie użycie (w % dla CPU)

13. Wymagana możliwość dostępu do historycznych danych wydajnościowych z poziomu GUI urządzenia do co najmniej 2 lat wstecz lub jako równoważne dostarczenie fizycznego serwera z oprogramowaniem umożliwiającym zbieranie i przeglądanie danych historycznych. Jeżeli do obsługi tej funkcjonalności wymagane są dodatkowe licencje, ich dostarczenie jest wymagane na tym etapie postępowania.

14. Wymagany dostęp do informacji o wykorzystanej fizycznej przestrzeni oraz aktualnym współczynniku redukcji danych. Jeżeli do obsługi tej funkcjonalności wymagane są dodatkowe licencje, ich dostarczenie jest wymagane na tym etapie postępowania.

15. Wymagane wsparcie dla Multi-factor authentication. Jeżeli do obsługi tej funkcjonalności wymagane są dodatkowe licencje, ich dostarczenie jest wymagane na tym etapie postępowania.

16. Wymagana możliwość definiowania polityk logowania. Jeżeli do obsługi tej funkcjonalności wymagane są dodatkowe licencje, ich dostarczenie jest wymagane na tym etapie postępowania.

17. Urządzenie musi deduplikować dane inline przed zapisem na nośnik dyskowy. Technologia deduplikacji musi wykorzystywać algorytm bazujący na zmiennym bloku. Algorytm ten musi samoczynnie i automatycznie dopasowywać się do otrzymywanego strumienia danych. Proces deduplikacji musi odbywać się inline – w pamięci urządzenia, przed zapisem danych na nośnik dyskowy. Dane muszą być poddane także procesowi kompresji. Jeżeli do obsługi powyższych funkcjonalności wymagane są dodatkowe licencje, należy je dostarczyć dla całej pojemności urządzenia.

18. Wymagana także obsługa deduplikacji na źródle, co pozwala ograniczyć zużycie sieci. Dostarczenie tej funkcjonalności jest wymagane na tym etapie postępowania.

19. Musi być oficjalne wsparcie producenta dla oferowanego deduplikatora maksymalnego stopnia redukcji danych co najmniej 65:1. Dostarczenie tej funkcjonalności jest wymagane na tym etapie postępowania.

20. Wymagana możliwość skonfigurowania tzw. quoty ograniczającej wystawione zasoby plikowe. Wymagana możliwość ograniczenia użytkownikom przestrzeni z której mogą korzystać lub liczby plików jakie mogą być przechowywane na udostępnionej przestrzeni. Dostarczenie tej funkcjonalności jest wymagane na tym etapie postępowania.

21. Wymagana możliwość ograniczenia dostępu do udostępnionych udziałów CIFS/NFS poprzez zdefiniowanie adresów IP lub ich przedziałów, które będą miały do nich dostęp. Dostarczenie tej funkcjonalności jest wymagane na tym etapie postępowania.

22. Tworzenie na żądanie tzw. migawkowej kopii danych (ang. snapshot) file system’ów w ramach deduplikatora do wykorzystania w celu np. wykonywania kopii zapasowych. Wymagana jest możliwość utworzenia harmonogramu snapshotów, które będą zabezpieczone przed modyfikacją oraz usunięciem przez wybrany okres czasu bez odpowiednich uprawnień celem przywrócenia danych w przypadku ataku ransomware. Musi być możliwość odtworzenia danych z dowolnej kopii (snapshot) wykonanej w ramach harmonogramu. Odtworzenie danych z jednej kopii nie może uniemożliwiać odtworzenia danych z innej kopii z innego punktu w czasie. Dostarczenie tej funkcjonalności jest wymagane na tym etapie postępowania na całą przestrzeń dyskową i na maksymalną liczbę snapshotów obsługiwanych przez oferowany model deduplikatora.

23. Wymagana możliwość zablokowania plików przed modyfikacją lub usunięciem (WORM) na poziomie całego file system’u. Dostarczenie licencji na tą funkcjonalność jest wymagane na tym etapie postępowania.

24. Urządzenie musi umożliwiać replikację danych do drugiego urządzenia w ramach tej samej rodziny oferowanego deduplikatora. Replikacja musi się odbywać w trybie asynchronicznym. Wymagana możliwość ograniczenia ilości przesyłanych danych poprzez ich deduplikację oraz kompresję. Dostarczenie tej funkcjonalności nie jest wymagane na tym etapie postępowania.

25. Deduplikator musi umożliwiać konfigurację harmonogramu replikacji poprzez określenie interwału (np. replikacja co 60min) lub konkretnych okien czasowych (np. w każdą sobotę o godz 20:00). Dostarczenie tej funkcjonalności nie jest wymagane na tym etapie postępowania.

26. Urządzenie musi wspierać co najmniej następujące aplikacje do backupu: Commvault, Veritas NetBackup, Veeam Backup&Replication.

27. Deduplikator musi posiadać możliwość upgrade’u firmware-u kontrolerów bez przerywania dostępu do danych.

28. Urządzenie przystosowane do napraw w miejscu instalacji oraz wymiany elementów bez konieczności jego wyłączania.

29. Urządzenie musi umożliwiać zdalne zarządzanie.

30. Urządzenie musi być fabrycznie nowe, wyprodukowane nie wcześniej niż 6 miesięcy przed datą dostarczenia do Zamawiającego i musi być objęte serwisem producenta lub autoryzowanego partnera serwisowego na terenie RP.

31. Urządzenie musi być zakupione w oficjalnym kanale dystrybucyjnym producenta. Na wezwanie Zamawiającego należy dostarczyć oświadczenie producenta oferowanego deduplikatora, potwierdzające pochodzenie urządzenia z oficjalnego kanału dystrybucyjnego producenta.

32. Wymagana gwarancja na 36 miesięcy w trybie 9x5 NBD.

33. W przypadku awarii, uszkodzone dyski pozostają u Zamawiającego tj. Zamawiający wymaga dostarczenia disk retention.

34. Na wezwanie Zamawiającego należy dostarczyć oświadczenie producenta z potwierdzeniem zaoferowanego poziomu gwarancji.

35. Zakres prac wdrożeniowych:

a. Opracowanie planu wdrożenia.

b. Instalacja deduplikatora wraz z wymaganymi licencjami i oprogramowaniem.

c. Konfiguracja deduplikatora zgodnie z wymaganiami zamawiającego.

d. Integracja z istniejącymi systemami IT zamawiającego.

e. Przeprowadzenie testów funkcjonalnych i wydajnościowych wymaganych przez Zamawiającego potwierdzających zadeklarowane funkcjonalności. Wynik negatywny jakiejkolwiek funkcjonalności lub testu pozwala Zamawiającemu odrzucić proponowaną ofertę i odstąpić od umowy bez podania przyczyny.

f. Weryfikacja poprawności działania deduplikatora.

**III. UTM – 1 szt.**

Przedmiotem zamówienia jest zakup urządzenia UTM z licencją zawierającą IPS, Advanced Malware Protection Service, Application Control, filtr URL, filtr DNS, filtr Video oraz Antispam na rok.

Wymagania:

1. Urządzenie klasy UTM (Unified Threat Management) z funkcjami NGFW (Next-Generation Firewall).

2. Sprzętowa akceleracja operacji sieciowych i bezpieczeństwa.

3. Obsługa minimum 28 portów Ethernet:

a. Co najmniej 2 porty 10 GE SFP+

b. Co najmniej 18 portów 1 GE RJ-45

c. Co najmniej 8 portów 1 GE SFP

4. Wydajność zapory ogniowej (Firewall Throughput) min. 20 Gbps.

5. Wydajność NGFW min. 1.5 Gbps.

6. Wydajność IPS min. 2.5 Gbps.

7. Wydajność ochrony przed zagrożeniami (Threat Protection) min. 1 Gbps.

8. Obsługa co najmniej 1 500 000 jednoczesnych sesji.

9. Maksymalna liczba nowych sesji na sekundę: min. 55 000.

10. Obsługa min. 2000 tuneli VPN IPsec.

11. Obsługa min. 500 użytkowników SSL VPN.

12. Stateful firewall z inspekcją pakietów.

13. Ochrona przed atakami DDoS, IPS (Intrusion Prevention System).

14. Wbudowany system wykrywania i zapobiegania włamaniom (IPS).

15. Zaawansowana ochrona przed zagrożeniami (sandboxing, wykrywanie exploitów).

16. Wbudowana ochrona antywirusowa i antymalware.

17. Filtracja treści WWW (Web Filtering) oraz ochrona poczty e-mail.

18. Obsługa uwierzytelniania dwuskładnikowego (2FA).

19. Obsługa VLAN, segmentacji sieci i polityk dostępu.

20. Obsługa tuneli VPN: IPsec, SSL VPN, L2TP.

21. Obsługa MFA (Multi-Factor Authentication) dla użytkowników VPN.

22. Szyfrowanie AES-256, SHA-256.

23. Możliwość stosowania polityk dostępu dla użytkowników VPN.

24. Możliwość zarządzania przez interfejs graficzny (GUI) oraz CLI.

25. Możliwość zdalnego monitorowania przez SNMP, Syslog.

26. Generowanie raportów bezpieczeństwa i aktywności sieciowej.

27. Wdrożenie w architekturze wysokiej dostępności (HA – High Availability).

28. Wsparcie techniczne producenta przez minimum rok.

29. Dostęp do aktualizacji zabezpieczeń przez min. rok.

30. Licencja na pełen pakiet usług UTM:

a. IPS,

b. Antywirus,

c. Sandboxing,

d. Antyspam,

e. Application Control

f. Advanced Malware Protection Service

g. filtr URL

h. filtr DNS

i. filtr Video

31. Możliwość pobierania aktualizacji firmware i bazy sygnatur zagrożeń.

**IV. UPS centralny – 1 szt.**

Przedmiotem zamówienia jest dostawa, instalacja oraz konfiguracja 1 szt. UPS centralnego.

Wymagania:

1. MOC min. 20000VA/18000W

2. Obudowa Tower

3. Maksymalna wysokość/głębokość rozwiązania: 1600mm/850mm (dotyczy zarówno jednostki zasilającej jak i szaf bateryjnych)

4. Waga modułu UPS: max. 90 kg.

5. Kolorowy wyświetlacz LCD z panelem dotykowym

6. Topologia podwójnej konwersji online

7. Kształt napięcia w trybie bateryjnym: Czyste napięcie sinusoidalne

8. Trójfazowa konstrukcja wejścia/wyjścia

9. Efektywność trybu ECO online do 98%

10. Wejściowy prąd znamionowy: min. 28 A

11. THDI <3% (Full Linear Load)

12. Współczynnik mocy wejściowej: 0.99

13. Tolerancja napięcia wyjściowego: 1.5%

14. Tolerancja napięcia w trybie ECO: ± 10%

15. Współczynnik szczytu: 3 : 1

16. Zniekształcenia harmoniczne (obciążenie liniowe): THD＜1%

17. Zniekształcenia harmoniczne (obciążenie nieliniowe): THD＜5.5%

18. Czas przełączania 0 ms

19. Konstrukcja z dwoma wejściami umożliwiając podłączenie jednego wejścia ze źródła zasilania prądem przemiennym i drugiego wejścia z innego źródła zasilania.

20. Serwisowy przełącznik obejściowy do płynnego przełączania zasilania na źródło sieciowe w trybie obejścia.

21. Kompatybilność z generatorem z wbudowaną funkcją automatycznej regulacji napięcia (AVR) do stabilizacji niestabilnych poziomów napięcia prądu z generatora.

22. Zgodne typy baterii: VRLA, AGM, Gel

23. Czas podtrzymania systemu min. 8 minut dla mocy 16 kW

24. Możliwość wydłużenia czasu podtrzymania przez dołożenie zestawów bateryjnych dostarczonych w zamkniętych szafach.

25. Możliwość ładowania szaf bateryjnych z mocą do 20% mocy UPS.

26. Możliwość pracy równoległej.

27. Możliwość łączenia równoległego do min. 4 jednostek UPS

28. Gniazdo wyjściowe: Kostka zaciskowa do łączenia przewodów

29. Złącze wejściowe: Kostka zaciskowa do łączenia przewodów

30. Porty komunikacyjne: RS232, RS485, SNMP, EPO, Dry contact

31. Zdalna komunikacja po protokole SNMP oraz http

32. Oprogramowanie w języku polskim do zarządzania UPSem z możliwością monitorowania zużycia energii oraz współpracy ze środowiskiem VMware ESXi 8.0 U2

33. Certyfikaty CE, IEC62040-1, IEC62040-2.

34. Gwarancja min. 24 miesiące.

35. Na wezwanie Zamawiającego należy dostarczyć oświadczenie producenta z potwierdzeniem zaoferowanego poziomu gwarancji.

36. Urządzenie i oprogramowanie muszą być zakupione w oficjalnym kanale dystrybucyjnym producenta. Na wezwanie Zamawiającego należy dostarczyć oświadczenie producenta oferowanego UPSa, potwierdzające pochodzenie urządzenia i oprogramowania z oficjalnego kanału dystrybucyjnego producenta.

37. Zakres prac wdrożeniowych:

a. Opracowanie planu wdrożenia.

b. Wdrożenie i konfiguracja:

i. Instalacja UPS i zestawów bateryjnych oraz podłączenie do sieci.

ii. Konfiguracja UPS zgodnie z wymaganiami zamawiającego.

iii. Integracja UPS z agregatem będącym przedmiotem tego postępowania oraz istniejącymi systemami IT zamawiającego.

c. Testy akceptacyjne:

i. Przeprowadzenie testów funkcjonalnych i wydajnościowych wymaganych przez Zamawiającego potwierdzających zadeklarowane funkcjonalności. Wynik negatywny jakiejkolwiek funkcjonalności lub testu pozwala Zamawiającemu odrzucić proponowaną ofertę i odstąpić od umowy bez podania przyczyny.

ii. Weryfikacja poprawności działania UPS oraz zestawów bateryjnych

**V. Oprogramowanie do backupu – 1 kpl.**

Przedmiotem zamówienia jest dostawa oprogramowania do tworzenia kopii zapasowych oraz przywracania danych. W ramach zamówienia przewiduje się zakup licencji wieczystych na oprogramowanie umożliwiające kompleksowe zarządzanie procesem backupu oraz przywracania danych dla 40 instancji ze wsparciem technicznym na minimum 12 miesięcy. Oprogramowanie ma zapewniać niezawodność, skalowalność oraz pełną integrację z istniejącą infrastrukturą zamawiającego. W celu weryfikacji funkcjonalności oferowanych przez proponowany system, Zamawiający zastrzega sobie możliwość wezwania do przeprowadzenia wybranych testów funkcjonalnych potwierdzających zadeklarowane funkcjonalności w ciągu 5 dni od daty wezwania. W razie odmowy przeprowadzenia testów lub ich wynik negatywny - pozwala Zamawiającemu odrzucić proponowaną ofertę bez podania przyczyny.

Wymagania:

1. Oprogramowanie musi współpracować z infrastrukturą VMware w wersji 7.x i 8 i nowszymi oraz Microsoft Hyper-V 2019 i 2022 i nowszymi. Wszystkie funkcjonalności w specyfikacji muszą być dostępne na wszystkich wspieranych platformach wirtualizacyjnych, chyba, że wyszczególniono inaczej.

2. 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.

3. Oprogramowanie musi być niezależne sprzętowo i umożliwiać wykorzystanie dowolnej platformy serwerowej i dyskowej.

4. Oprogramowanie musi tworzyć “samowystarczalne” archiwa do odzyskania których niewymagana jest osobna baza danych z metadanymi deduplikowanych bloków.

5. 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.

6. 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.

7. 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.

8. 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.

9. Oprogramowanie musi wspierać niezmienność kopii zapasowych na potrzeby ochrony przed ransomware poprzez niedopuszczenie do usunięcia lub modyfikacji kopii zapasowej w zadanym okresie czasu.

10. Oprogramowanie nie może instalować żadnych stałych agentów wymagających wdrożenia czy upgradowania wewnątrz maszyny wirtualnej dla jakichkolwiek funkcjonalności backupu lub odtwarzania.

11. 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).

12. Oprogramowanie musi zapewniać możliwość delegacji uprawnień do odtwarzania na portalu.

13. Oprogramowanie musi mieć możliwość integracji z innymi systemami poprzez wbudowane RESTful API.

14. Oprogramowanie musi mieć wbudowane mechanizmy backupu konfiguracji w celu prostego odtworzenia systemu po całkowitej reinstalacji.

15. 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.

16. Oprogramowanie musi posiadać mechanizmy chroniące przed utratą hasła szyfrowania.

17. Oprogramowanie musi posiadać architekturę klient/serwer z możliwością instalacji wielu instancji konsoli administracyjnych.

18. Oprogramowanie musi posiadać natywne mechanizmy uwierzytelniania wieloskładnikowego (MFA) w celu dostępu do konsoli administracyjnej.

19. Oprogramowanie musi wykorzystywać mechanizmy Change Block Tracking na wszystkich wspieranych platformach wirtualizacyjnych. Mechanizmy muszą być certyfikowane przez dostawcę platformy wirtualizacyjnej.

20. Oprogramowanie musi wykorzystywać mechanizmy śledzenia zmienionych plików przy zabezpieczaniu udziałów plikowych.

21. 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.

22. 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.

23. Oprogramowanie musi posiadać wsparcie dla VMware vSAN potwierdzone odpowiednią certyfikacją Vmware.

24. Oprogramowanie musi wspierać kopiowanie backupów oraz zasobów plikowych na taśmy.

25. Oprogramowanie musi mieć możliwość tworzenia retencji GFS (Grandfather-Father-Son).

26. Oprogramowanie musi wspierać bezpośrednią integrację z urządzeniami deduplikacyjnymi. Minimalnie wsparcie wymagane dla Dell DataDomain, HPE StoreOnce, ExaGrid, Fujitsu CS800, Quantum DXi oraz Infinidat InfiniGuard.

27. Oprogramowanie musi wspierać BlockClone API w przypadku użycia Windows Server 2019 lub 2022 z systemem pliku ReFS jako repozytorium backupu. Podobna funkcjonalność musi być zapewniona dla repozytoriów opartych o linuxowy system plików XFS.

28. Oprogramowanie musi mieć możliwość kopiowania backupów oraz replikacji wirtualnych maszyn z wykorzystaniem wbudowanej akceleracji WAN.

29. 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.

30. 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.

31. Oprogramowanie musi umożliwiać przechowywanie punktów przywracania dla replik.

32. Oprogramowanie musi umożliwiać wykorzystanie istniejących w infrastrukturze wirtualnych maszyn jako źródła do dalszej replikacji (replica seeding).

33. Oprogramowanie musi wykorzystywać wszystkie oferowane przez hypervisor tryby transportu (sieć, hot-add, LAN Free-SAN).

34. 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.

35. 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).

36. 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.

37. Oprogramowanie musi pozwalać na zaprezentowanie pojedynczego dysku bezpośrednio z kopii zapasowej do wybranej działającej maszyny wirtualnej vSpehre.

38. 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.

39. Oprogramowanie musi umożliwiać pełne odtworzenie wirtualnej maszyny, plików konfiguracji i dysków.

40. Oprogramowanie musi umożliwiać pełne odtworzenie wirtualnej maszyny bezpośrednio do Microsoft Azure, Microsoft Azure Stack, Amazon EC2 oraz Google Cloud Platform.

41. 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.

42. 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.

43. Oprogramowanie musi wspierać odtwarzanie pojedynczych plików z systemów Windows, Linux, BSD, Solaris, Mac, Novell

44. Oprogramowanie musi wspierać przywracanie plików z partycji Linux LVM oraz Windows Storage Spaces.

45. Oprogramowanie musi umożliwiać szybkie granularne odtwarzanie obiektów aplikacji bez użycia jakiegokolwiek agenta zainstalowanego wewnątrz maszyny wirtualnej.

46. 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.

47. 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.

48. 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.

49. 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.

50. 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.

51. 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.

52. Oprogramowanie musi posiadać natywną integrację dla backupów wykonywanych poprzez Oracle RMAN

53. Oprogramowanie musi posiadać natywną integrację dla backupów wykonywanych poprzez SAP HANA, SAP Oracle

54. Oprogramowanie musi posiadać natywną integrację dla backupów wykonywanych poprzez MS SQL VDI

55. Oprogramowanie musi wspierać także specyficzne metody odtwarzania w tym "reverse CBT" oraz odtwarzanie z wykorzystaniem sieci SAN

56. 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)

57. Dla VMware’a oprogramowanie musi pozwalać na uruchomienie takiego środowiska dla replik maszyn wirtualnych oraz bezpośrednio ze snapshotów macierzowych stworzonych na wspieranych urządzeniach.

58. 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

59. 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.

60. Oprogramowanie musi umożliwiać dwuetapowe, automatyczne, odtwarzanie maszyn wirtualnych z możliwością wstrzyknięcia dowolnego skryptu przed odtworzeniem danych do środowiska produkcyjnego.

61. Zaoferowane licencje nie mogą mieć żadnych ograniczeń czasowych (muszą być wieczyste) dla wszystkich wymaganych funkcjonalności backupowych

62. Zaoferowane oprogramowanie musi być licencjonowane per ilość maszyn wirtualnych podlegających backupowi niezależnie czy będą wykorzystywani agenci plikowi czy bazodanowi zainstalowani wewnątrz maszyny.

63. Zaoferowane licencje na system muszą zapewnić backup danych z 40 instancji.

64. Oprogramowanie musi być zakupione w oficjalnym kanale dystrybucyjnym producenta.

65. Zamawiający wymaga licencji wieczystych z gwarancją i serwisem na okres minimum 24 miesięcy, z możliwością przedłużenia. Serwis powinien obejmować wsparcie techniczne, usuwanie usterek oraz aktualizacje oprogramowania.

66. Oświadczenie producenta z potwierdzeniem zaoferowanego poziomu gwarancji.

67. Wdrożenie:

a. Opracowanie szczegółowego planu wdrożenia.

b. Instalacja i konfiguracja oprogramowania do backupu wskazanych instancji.

c. Konfiguracja polityk bezpieczeństwa zgodnie z wymaganiami zamawiającego.

d. Testy funkcjonalne systemu.

e. Dostarczenie pełnej dokumentacji powykonawczej w języku polskim.

**VI. Oprogramowanie do zbierania logów z infrastruktury sieciowej – 1 kpl.**

Przedmiot zamówienia dotyczy dostawy, instalacji, konfiguracji oraz wdrożenia rozbudowanego systemu bezpieczeństwa informatycznego, który integruje różnorodne funkcje monitorowania, analizy oraz reakcji na zagrożenia w celu kompleksowej ochrony infrastruktury IT. System musi bazować na nowoczesnych technologiach klasy SIEM (Security Information and Event Management), a także umożliwia holistyczne podejście do bezpieczeństwa oraz zarządzanie incydentami w sposób wysoce zautomatyzowany i skalowalny. Zamówienie obejmuje dostawę licencji wieczystej ze wsparciem technicznym na minimum 24 miesiące. W celu weryfikacji funkcjonalności oferowanych przez proponowane oprogramowanie, Zamawiający zastrzega sobie możliwość wezwania do przeprowadzenia wybranych testów funkcjonalnych potwierdzających zadeklarowane funkcjonalności w ciągu 5 dni od daty wezwania. W razie odmowy przeprowadzenia testów lub ich wynik negatywny - pozwala Zamawiającemu odrzucić proponowaną ofertę bez podania przyczyny.

Wymagania:

1. System musi gromadzić dane z różnorodnych źródeł, takich jak:

a. Logi systemowe (systemów operacyjnych, serwerów, aplikacji, urządzeń sieciowych).

b. Informacje o zdarzeniach (np. próby logowania, zmiany uprawnień, działania użytkowników).

c. Dane dotyczące konfiguracji infrastruktury IT (np. plików konfiguracyjnych, polityk bezpieczeństwa).

2. System musi automatycznie analizować te dane w czasie rzeczywistym, identyfikując potencjalne zagrożenia oraz anomalie na podstawie wcześniej zdefiniowanych reguł, sygnatur oraz zaawansowanych algorytmów analitycznych.

3. Kluczową funkcją systemu musi być ciągłe monitorowanie stanu bezpieczeństwa w czasie rzeczywistym. System musi umożliwiać:

a. Wczesne wykrywanie zagrożeń: Wykorzystanie analizy behawioralnej oraz sztucznej inteligencji do identyfikacji nietypowych zachowań użytkowników, urządzeń i aplikacji.

b. Pełna widoczność nad wszystkimi elementami infrastruktury IT, w tym także nad środowiskami wirtualnymi i chmurowymi.

c. Analiza historyczna zdarzeń: System musi umożliwiać retrospektywne badanie logów i zdarzeń, co jest niezbędne do dochodzeń powłamaniowych i audytów bezpieczeństwa.

4. System musi posiadać zaawansowane wykrywanie zagrożeń w różnych środowiskach, takich jak:

a. Środowiska chmurowe (AWS, Azure, Google Cloud).

b. Kontenery (Docker, Kubernetes).

c. Urządzenia końcowe.

5. System musi rozszerzać możliwości SIEM, pozwalając na:

a. Skoordynowane wykrywanie zagrożeń w całym środowisku IT.

b. Szybkie reagowanie na incydenty dzięki integracji z innymi narzędziami do zarządzania i automatyzacji (np. firewalle, narzędzia do zarządzania zasobami IT).

c. Automatyzację działań naprawczych, co redukuje czas reakcji na zagrożenia oraz minimalizuje ryzyko.

6. System musi wspierać zarządzanie incydentami bezpieczeństwa poprzez:

a. Automatyczne powiadomienia o wykrytych zagrożeniach, pozwalające administratorom na szybkie podjęcie działań.

b. Raportowanie incydentów z pełnym zestawem informacji potrzebnych do analizy i dalszych działań naprawczych.

c. Korelowanie zdarzeń z różnych źródeł w celu lepszego zrozumienia zagrożeń i zidentyfikowania ich źródła.

7. System musi pomagać organizacji w utrzymywaniu zgodności z regulacjami prawnymi i standardami bezpieczeństwa poprzez:

a. Monitorowanie działań użytkowników i zapis zmian w systemach, co pozwala na śledzenie operacji oraz wykrywanie nieautoryzowanych działań.

b. Automatyczne generowanie raportów audytowych i zgodności, które można przedstawić audytorom oraz organom nadzoru.

c. Tworzenie alertów zgodności, które informują o potencjalnych naruszeniach polityk bezpieczeństwa.

8. System musi oferować wysoką skalowalność oraz zapewniać integrację z szeroką gamą innych rozwiązań i narzędzi używanych w ramach zabezpieczeń IT.

9. Zakres prac wdrożeniowych:

a. Opracowanie szczegółowego planu wdrożenia.

b. Instalacja i konfiguracja:

i. Instalacja i konfiguracja oprogramowania na serwerze.

ii. Konfiguracja polityk bezpieczeństwa zgodnie z wymaganiami zamawiającego.

iii. Testy funkcjonalne systemu.

c. Dostarczenie pełnej dokumentacji powykonawczej w języku polskim.

**VII. Oprogramowanie antywirusowe z XDR – 1 kpl.**

Przedmiotem zamówienia jest dostawa, wdrożenie i konfiguracja oprogramowania antywirusowego z XDR. Oprogramowanie będzie musiało spełniać wymogi operacyjne i technologiczne Zamawiającego, zapewniając pełną integrację z istniejącą infrastrukturą oraz optymalizację działań związanych z cyberbezpieczeństwem. Zamówienie obejmuje dostawę licencji na 35 stanowisk na okres minimum 24 miesiące. W celu weryfikacji funkcjonalności oferowanych przez proponowane oprogramowanie, Zamawiający zastrzega sobie możliwość wezwania do przeprowadzenia wybranych testów funkcjonalnych potwierdzających zadeklarowane funkcjonalności w ciągu 5 dni od daty wezwania. W razie odmowy przeprowadzenia testów lub ich wynik negatywny - pozwala Zamawiającemu odrzucić proponowaną ofertę bez podania przyczyny.

Wymagania:

1. Administracja zdalna w chmurze:

a. Rozwiązanie musi być dostępne w chmurze producenta oprogramowania antywirusowego.

b. Rozwiązanie musi umożliwiać dostęp do konsoli centralnego zarządzania z poziomu interfejsu WWW.

c. Rozwiązanie musi być zabezpieczone za pośrednictwem protokołu SSL.

d. Rozwiązanie musi posiadać mechanizm wykrywający sklonowane maszyny na podstawie unikatowego identyfikatora sprzętowego stacji.

e. Rozwiązanie musi posiadać możliwość komunikacji agenta przy wykorzystaniu HTTP Proxy.

f. Rozwiązanie musi posiadać możliwość zarządzania urządzeniami mobilnymi – MDM.

g. Rozwiązanie musi posiadać możliwość wymuszenia dwufazowej autoryzacji podczas logowania do konsoli administracyjnej.

h. Rozwiązanie musi posiadać możliwość dodania zestawu uprawnień dla użytkowników w oparciu co najmniej o funkcje zarządzania: politykami, raportowaniem, zarządzaniem licencjami, zadaniami administracyjnymi. Każda z funkcji musi posiadać możliwość wyboru uprawnienia: odczyt, użyj, zapisz oraz brak.

i. Rozwiązanie musi posiadać minimum 80 szablonów raportów, przygotowanych przez producenta.

j. Rozwiązanie musi posiadać możliwość tworzenia grup statycznych i dynamicznych komputerów.

k. Grupy dynamiczne muszą być tworzone na podstawie szablonu określającego warunki, jakie musi spełnić klient, aby został umieszczony w danej grupie. Warunki muszą zawierać co najmniej: adresy sieciowe IP, aktywne zagrożenia, stan funkcjonowania/ochrony, wersja systemu operacyjnego, podzespoły komputera.

l. Rozwiązanie musi posiadać możliwość uruchomienia zadań automatycznie, przynajmniej z wyzwalaczem: wyrażenie CRON, codziennie, cotygodniowo, comiesięcznie, corocznie, po wystąpieniu nowego zdarzenia oraz umieszczeniu agenta w grupie dynamicznej.

2. Ochrona stacji roboczych:

a. Rozwiązanie musi wspierać systemy operacyjne Windows (Windows 10/Windows 11).

b. Rozwiązanie musi wspierać architekturę ARM64.

c. Rozwiązanie musi zapewniać wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor.

d. Rozwiązanie musi posiadać wbudowaną technologię do ochrony przed rootkitami oraz podłączeniem komputera do sieci botnet.

e. Rozwiązanie musi zapewniać wykrywanie potencjalnie niepożądanych, niebezpiecznych oraz podejrzanych aplikacji.

f. Rozwiązanie musi zapewniać skanowanie w czasie rzeczywistym otwieranych, zapisywanych i wykonywanych plików.

g. Rozwiązanie musi zapewniać skanowanie całego dysku, wybranych katalogów lub pojedynczych plików "na żądanie" lub według harmonogramu.

h. Rozwiązanie musi zapewniać skanowanie plików spakowanych i skompresowanych oraz dysków sieciowych i dysków przenośnych.

i. Rozwiązanie musi posiadać opcję umieszczenia na liście wykluczeń ze skanowania wybranych plików, katalogów lub plików na podstawie rozszerzenia, nazwy, sumy kontrolnej (SHA1) oraz lokalizacji pliku.

j. Rozwiązanie musi zapewniać skanowanie i oczyszczanie poczty przychodzącej POP3 i IMAP „w locie” (w czasie rzeczywistym), zanim zostanie dostarczona do klienta pocztowego, zainstalowanego na stacji roboczej (niezależnie od konkretnego klienta pocztowego).

k. Rozwiązanie musi zapewniać skanowanie ruchu sieciowego wewnątrz szyfrowanych protokołów HTTPS, POP3S, IMAPS.

l. Rozwiązanie musi posiadać wbudowane dwa niezależne moduły heurystyczne – jeden wykorzystujący pasywne metody heurystyczne i drugi wykorzystujący aktywne metody heurystyczne oraz elementy sztucznej inteligencji. Musi istnieć możliwość wyboru, z jaką heurystyka ma odbywać się skanowanie – z użyciem jednej lub obu metod jednocześnie.

m. Rozwiązanie musi zapewniać blokowanie zewnętrznych nośników danych na stacji w tym przynajmniej: Pamięci masowych, optycznych pamięci masowych, pamięci masowych Firewire, urządzeń do tworzenia obrazów, drukarek USB, urządzeń Bluetooth, czytników kart inteligentnych, modemów, portów LPT/COM oraz urządzeń przenośnych.

n. Rozwiązanie musi posiadać funkcję blokowania nośników wymiennych, bądź grup urządzeń ma umożliwiać użytkownikowi tworzenie reguł dla podłączanych urządzeń minimum w oparciu o typ, numer seryjny, dostawcę lub model urządzenia.

o. Moduł HIPS musi posiadać możliwość pracy w jednym z pięciu trybów:

i. tryb automatyczny z regułami, gdzie program automatycznie tworzy i wykorzystuje reguły wraz z możliwością wykorzystania reguł utworzonych przez użytkownika,

ii. tryb interaktywny, w którym to rozwiązanie pyta użytkownika o akcję w przypadku wykrycia aktywności w systemie,

iii. tryb oparty na regułach, gdzie zastosowanie mają jedynie reguły utworzone przez użytkownika,

iv. tryb uczenia się, w którym rozwiązanie uczy się aktywności systemu i użytkownika oraz tworzy odpowiednie reguły w czasie określonym przez użytkownika. Po wygaśnięciu tego czasu program musi samoczynnie przełączyć się w tryb pracy oparty na regułach,

v. tryb inteligentny, w którym rozwiązanie będzie powiadamiało wyłącznie o szczególnie podejrzanych zdarzeniach.

p. Rozwiązanie musi być wyposażone we wbudowaną funkcję, która wygeneruje pełny raport na temat stacji, na której zostało zainstalowane, w tym przynajmniej z:

i. zainstalowanych aplikacji

ii. usług systemowych

iii. informacji o systemie operacyjnym i sprzęcie

iv. aktywnych procesów i połączeń sieciowych

v. harmonogramu systemu operacyjnego

vi. pliku hosts

vii. sterowników.

q. Funkcja, generująca taki log, ma posiadać przynajmniej 9 poziomów filtrowania wyników pod kątem tego, które z nich są podejrzane dla rozwiązania i mogą stanowić zagrożenie bezpieczeństwa.

r. Rozwiązanie musi posiadać automatyczną, inkrementacyjną aktualizację silnika detekcji.

s. Rozwiązanie musi posiadać tylko jeden proces uruchamiany w pamięci, z którego korzystają wszystkie funkcje systemu (antywirus, antyspyware, metody heurystyczne).

t. Rozwiązanie musi posiadać funkcjonalność skanera UEFI, który chroni użytkownika poprzez wykrywanie i blokowanie zagrożeń, atakujących jeszcze przed uruchomieniem systemu operacyjnego.

u. Rozwiązanie musi posiadać ochronę antyspamową dla programów pocztowych MS Outlook.

v. Zapora osobista rozwiązania musi pracować w jednym z czterech trybów:

i. tryb automatyczny – rozwiązanie blokuje cały ruch przychodzący i zezwala tylko na połączenia wychodzące,

ii. tryb interaktywny – rozwiązanie pyta się o każde nowo nawiązywane połączenie,

iii. tryb oparty na regułach – rozwiązanie blokuje cały ruch przychodzący i wychodzący, zezwalając tylko na połączenia skonfigurowane przez administratora,

iv. tryb uczenia się – rozwiązanie automatycznie tworzy nowe reguły zezwalające na połączenia przychodzące i wychodzące. Administrator musi posiadać możliwość konfigurowania czasu działania trybu.

w. Rozwiązanie musi być wyposażona w moduł bezpiecznej przeglądarki.

x. Przeglądarka musi automatycznie szyfrować wszelkie dane wprowadzane przez Użytkownika.

y. Praca w bezpiecznej przeglądarce musi być wyróżniona poprzez odpowiedni kolor ramki przeglądarki oraz informację na ramce przeglądarki.

z. Rozwiązanie musi być wyposażone w zintegrowany moduł kontroli dostępu do stron internetowych.

aa. Rozwiązanie musi posiadać możliwość filtrowania adresów URL w oparciu o co najmniej 140 kategorii i podkategorii.

3. Ochrona serwera:

a. Rozwiązanie musi wspierać systemy Microsoft Windows Server 2012 i nowszych oraz Linux w tym co najmniej: RedHat Enterprise Linux (RHEL), CentOS, Ubuntu Server, Debian, SUSE Linux Enterprise Server (SLES), Oracle Linux oraz Amazon Linux.

b. Rozwiązanie musi zapewniać ochronę przed wirusami, trojanami, robakami i innymi zagrożeniami.

c. Rozwiązanie musi zapewniać wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor.

d. Rozwiązanie musi zapewniać możliwość skanowania dysków sieciowych typu NAS.

e. Rozwiązanie musi posiadać wbudowane dwa niezależne moduły heurystyczne – jeden wykorzystujący pasywne metody heurystyczne i drugi wykorzystujący aktywne metody heurystyczne oraz elementy sztucznej inteligencji. Rozwiązanie musi istnieć możliwość wyboru, z jaką heurystyka ma odbywać się skanowanie – z użyciem jednej lub obu metod jednocześnie.

f. Rozwiązanie musi wspierać automatyczną, inkrementacyjną aktualizację silnika detekcji.

g. Rozwiązanie musi posiadać możliwość wykluczania ze skanowania procesów.

h. Rozwiązanie musi posiadać możliwość określenia typu podejrzanych plików, jakie będą przesyłane do producenta, w tym co najmniej pliki wykonywalne, archiwa, skrypty, dokumenty.

4. Dodatkowe wymagania dla ochrony serwerów Windows:

a. Rozwiązanie musi posiadać możliwość skanowania plików i folderów, znajdujących się w usłudze chmurowej OneDrive.

b. Rozwiązanie musi posiadać system zapobiegania włamaniom działający na hoście (HIPS).

c. Rozwiązanie musi wspierać skanowanie magazynu Hyper-V.

d. Rozwiązanie musi posiadać funkcjonalność skanera UEFI, który chroni użytkownika poprzez wykrywanie i blokowanie zagrożeń, atakujących jeszcze przed uruchomieniem systemu operacyjnego.

e. Rozwiązanie musi zapewniać administratorowi blokowanie zewnętrznych nośników danych na stacji w tym przynajmniej: Pamięci masowych, optycznych pamięci masowych, pamięci masowych Firewire, urządzeń do tworzenia obrazów, drukarek USB, urządzeń Bluetooth, czytników kart inteligentnych, modemów, portów LPT/COM oraz urządzeń przenośnych.

f. Rozwiązanie musi automatyczne wykrywać usługi zainstalowane na serwerze i tworzyć dla nich odpowiednie wyjątki.

g. Rozwiązanie musi posiadać wbudowany system IDS z detekcją prób ataków, anomalii w pracy sieci oraz wykrywaniem aktywności wirusów sieciowych.

h. Rozwiązanie musi zapewniać możliwość dodawania wyjątków dla systemu IDS, co najmniej w oparciu o występujący alert, kierunek, aplikacje, czynność oraz adres IP.

i. Rozwiązanie musi posiadać ochronę przed oprogramowaniem wymuszającym okup za pomocą dedykowanego modułu.

5. Dodatkowe wymagania dla ochrony serwerów Linux:

a. Rozwiązanie musi pozwalać, na uruchomienie lokalnej konsoli administracyjnej, działającej z poziomu przeglądarki internetowej.

b. Lokalna konsola administracyjna nie może wymagać do swojej pracy, uruchomienia i instalacji dodatkowego rozwiązania w postaci usługi serwera Web.

c. Rozwiązanie, do celów skanowania plików na macierzach NAS / SAN, musi w pełni wspierać rozwiązanie Dell EMC Isilon.

d. 21. Rozwiązanie musi działać w architekturze bazującej na technologii mikro-serwisów. Funkcjonalność ta musi zapewniać podwyższony poziom stabilności, w przypadku awarii jednego z komponentów rozwiązania, nie spowoduje to przerwania pracy całego procesu, a jedynie wymusi restart zawieszonego mikro-serwisu.

6. Ochrona urządzeń mobilnych opartych o system Android:

a. Rozwiązanie musi zapewniać skanowanie wszystkich typów plików, zarówno w pamięci wewnętrznej, jak i na karcie SD, bez względu na ich rozszerzenie.

b. Rozwiązanie musi zapewniać co najmniej 2 poziomy skanowania: inteligentne i dokładne.

c. Rozwiązanie musi zapewniać automatyczne uruchamianie skanowania, gdy urządzenie jest w trybie bezczynności (w pełni naładowane i podłączone do ładowarki).

d. Rozwiązanie musi posiadać możliwość skonfigurowania zaufanej karty SIM.

e. Rozwiązanie musi zapewniać wysłanie na urządzenie komendy z konsoli centralnego zarządzania, która umożliwi:

i. usunięcie zawartości urządzenia,

ii. przywrócenie urządzenie do ustawień fabrycznych,

iii. zablokowania urządzenia,

iv. uruchomienie sygnału dźwiękowego,

v. lokalizację GPS.

f. Rozwiązanie musi zapewniać administratorowi podejrzenie listy zainstalowanych aplikacji.

g. Rozwiązanie musi posiadać blokowanie aplikacji w oparciu o:

i. nazwę aplikacji,

ii. nazwę pakietu,

iii. kategorię sklepu Google Play,

iv. uprawnienia aplikacji,

v. pochodzenie aplikacji z nieznanego źródła.

7. Szyfrowanie:

a. System szyfrowania danych musi wspierać instalację aplikacji klienckiej w środowisku Microsoft Windows 7/8/8.1/10 32-bit i 64-bit.

b. System szyfrowania musi wspierać zarządzanie natywnym szyfrowaniem w systemach macOS (FileVault).

c. Aplikacja musi posiadać autentykacje typu Pre-boot, czyli uwierzytelnienie użytkownika zanim zostanie uruchomiony system operacyjny. Musi istnieć także możliwość całkowitego lub czasowego wyłączenia tego uwierzytelnienia.

d. Aplikacja musi umożliwiać szyfrowanie danych tylko na komputerach z UEFI.

8. Moduł XDR:

a. Dostęp do konsoli centralnego zarządzania musi odbywać się z poziomu interfejsu WWW.

b. Serwer administracyjny musi posiadać możliwość wysyłania zdarzeń do konsoli administracyjnej tego samego producenta.

c. Interfejs musi być zabezpieczony za pośrednictwem protokołu SSL.

d. Serwer administracyjny musi posiadać możliwość wprowadzania wykluczeń, po których nie zostanie wyzwolony alarm bezpieczeństwa.

e. Wykluczenia muszą dotyczyć procesu lub procesu „rodzica”.

f. Utworzenie wykluczenia musi automatycznie rozwiązywać alarmy, które pasują do utworzonego wykluczenia.

g. Kryteria wykluczeń muszą być konfigurowane w oparciu o przynajmniej: nazwę procesu, ścieżkę procesu, wiersz polecenia, wydawcę, typ podpisu, SHA-1, nazwę komputera, grupę, użytkownika.

h. Serwer musi posiadać ponad 900 wbudowanych reguł, po których wystąpieniu, nastąpi wyzwolenie alarmu bezpieczeństwa. Administrator musi też posiadać możliwość utworzenia własnych reguł i edycji reguł dodanych przez producenta.

i. Serwer administracyjny musi oferować możliwość blokowania plików po sumach kontrolnych. W ramach blokady musi istnieć możliwość dodania komentarza oraz konfiguracji wykonywanej czynności, po wykryciu wprowadzonej sumy kontrolnej.

j. Administrator musi posiadać możliwość weryfikacji uruchomionych plików wykonywalnych na stacji roboczej z możliwością podglądu szczegółów wybranego procesu przynajmniej o: SHA-1, typ podpisu, wydawcę, opis pliku, wersję pliku, nazwę firmy, nazwę produktu, wersję produktu, oryginalną nazwę pliku, rozmiar pliku oraz reputację i popularność pliku.

k. Administrator, w ramach plików wykonywalnych oraz plików DLL, musi posiadać możliwość ich oznaczenia jako bezpieczne, pobrania do analizy oraz ich zablokowania.

l. Administrator musi posiadać możliwość weryfikacji uruchomionych skryptów na stacjach roboczych, wraz z informacją dotyczącą parametrów uruchomienia. Administrator musi posiadać możliwość oznaczenia skryptu jako bezpieczny lub niebezpieczny.

m. W ramach przeglądania wykonanego skryptu, administrator musi posiadać możliwość szczegółowego podglądu wykonanych przez skrypt czynności w formie tekstowej.

n. W ramach przeglądania wykonanego skryptu lub pliku exe, administrator musi posiadać możliwość weryfikacji powiązanych zdarzeń dotyczących przynajmniej: modyfikacji plików i rejestru, zestawionych połączeń sieciowych i utworzonych plików wykonywalnych.

o. Serwer administracyjny musi oferować możliwość przekierowania do konsoli zarządzającej produktu antywirusowego tego samego producenta, w celu weryfikacji szczegółów wybranej stacji roboczej. W konsoli zarządzającej produktu antywirusowego, administrator musi mieć możliwość podglądu informacji dotyczących przynajmniej: podzespołów zarządzanego komputera (w tym przynajmniej: producent, model, numer seryjny, informacje o systemie, procesor, peryferyjne, urządzenia audio, drukarki, karty sieciowe, urządzenia masowe) oraz wylistowanie zainstalowanego oprogramowania firm trzecich.

p. Konsola administracyjna musi mieć możliwość tagowania obiektów.

q. Konsola administracyjna musi umożliwiać połączenie się do stacji roboczej z możliwością wykonywania poleceń powershell.

9. Zamawiający wymaga licencji dla 35 stanowisk na okres minimum 24 miesiące, z możliwością przedłużenia. Licencja powinna obejmować wsparcie techniczne, usuwanie usterek oraz aktualizacje oprogramowania.

10. Oprogramowanie musi być zakupione w oficjalnym kanale dystrybucyjnym producenta. Na wezwanie Zamawiającego należy dostarczyć oświadczenie producenta oferowanego oprogramowania, potwierdzające pochodzenie oprogramowania z oficjalnego kanału dystrybucyjnego producenta.

**VIII. Oprogramowanie do zarządzania zasobami IT – 1 kpl.**

Przedmiotem zamówienia jest dostawa oprogramowania do zarządzania zasobami IT. Zamówienie obejmuje dostawę licencji wieczystej na 35 stanowisk ze wsparciem technicznym na minimum 24 miesiące. W celu weryfikacji funkcjonalności oferowanych przez proponowane oprogramowanie. Zamawiający zastrzega sobie możliwość wezwania do przeprowadzenia wybranych testów funkcjonalnych potwierdzających zadeklarowane funkcjonalności w ciągu 5 dni od daty wezwania. W razie odmowy przeprowadzenia testów lub ich wynik negatywny - pozwala Zamawiającemu odrzucić proponowaną ofertę bez podania przyczyny.

Wymagania:

1. Oprogramowanie musi posiadać polski oraz angielski interfejs językowy.

2. Oprogramowanie musi posiadać architekturę trójwarstwową składającą się z Bazy Danych, Serwera Aplikacji, Agenta/Konsoli zarządzającej.

3. Oprogramowanie musi umożliwiać obsługę dedykowanych kluczy szyfrujących podczas komunikacji pomiędzy agentami, serwer aplikacji i konsolą zarządzającą.

4. Odczyt informacji dotyczących parametrów sprzętowych komputera musi odbywać się za pośrednictwem agenta systemu instalowanego na komputerach użytkowników.

5. Agent systemu nie może nasłuchiwać na żadnym porcie sieciowym po stronie stanowiska komputerowego użytkownika.

6. Oprogramowanie musi umożliwiać wybór instalacji agenta w trybie standardowym oraz bezpiecznym tj. braku wkompilowanych funkcji takich jak zdalne zarządzanie, transfer plików, zdalny pulpit.

7. Oprogramowanie musi posiadać procedurę uwierzytelnienia i autoryzacji kont operatorów w konsoli zarządzającej poprzez fizyczne zabezpieczenie sprzętowe (lokalne lub sieciowe) wraz z hasłem, który umożliwia jednoczesną prace wielu administratorom. Logowanie użytkowników konsoli zarządzającej musi umożliwiać integrację z kontami Active Directory. Wymagane zabezpieczenie sprzętowe musi posiadać mechanizm szyfrowania danych AES w obrębie przechowywania danych wrażliwych.

8. Oprogramowanie musi posiadać dodatkową autoryzację użytkownika konsoli zarządzającej za pomocą usługi Google Authenticator oraz Microsoft Authenticator.

9. Oprogramowanie musi posiadać moduł zarządzania uprawnieniami do poszczególnych funkcjonalności systemu dla operatorów konsoli zarządzającej zgodny z modelem RBAC (Role Based Access Control).

10. Oprogramowanie musi umożliwiać nadawanie oraz odbieranie uprawnień w czasie rzeczywistym (brak konieczności przelogowania użytkownika konsoli systemu).

11. Oprogramowanie musi umożliwiać blokadę wybranych uprawnień konkretnego użytkownika niezależnie od uprawnień wynikających z przypisanych ról.

12. Oprogramowanie musi współpracować z serwerem MSSQL Server 2008R2-2019

13. Oprogramowanie, w zakresie wszystkich warstw, nie może wymagać do prawidłowej pracy komponentów Java.

14. Oprogramowanie serwera aplikacji musi posiadać funkcjonalność centralnego wysyłania wybranych powiadomień mailowych .

15. Oprogramowanie musi posiadać moduł zarządzania uprawnieniami do danych w zakresie wybranych jednostek organizacyjnych oraz typów zasobów poszczególnych użytkowników konsoli. Wszelkie raporty, zestawienia oraz funkcje obejmują wtedy tylko wynikowe obiekty.

16. Oprogramowanie musi być podpisane cyfrowo przez Producenta ważnym certyfikatem, z prawidłową ścieżką certyfikacji, w której główny urząd certyfikacji (Root CA) jest uczestnikiem programu certyfikatów głównych systemu Windows. Podpis cyfrowy dotyczy składników Producenta systemu w zakresie plików wykonywalnych (\*.exe), plików bibliotek współdzielonych (\*.dll), plików sterowników (\*.sys) oraz pakietów instalacyjnych oprogramowania (\*.msi).

17. Oprogramowanie agentów musi posiadać obsługę sesji terminalowych Windows.

18. Oprogramowanie musi zapewniać dowolną konfigurację pracy wszystkich agentów, jednostek organizacyjnych, pojedynczego agenta, poprzez dziedziczenie definiowanych przez administratora parametrów. Zmiany konfiguracji agentów następują w trybie natychmiastowym (online).

19. Oprogramowanie musi posiadać raport przedstawiający różnice w konfiguracji poszczególnych agentów w stosunku do konfiguracji globalnej.

20. Oprogramowanie musi posiadać mechanizm logowania zmian w konfiguracji agentów przez użytkowników konsoli (data, czas, login, poprzednia i nowa wartość).

21. Oprogramowanie musi posiadać mechanizm analizy czasu pracy komputera, informujący użytkownika (alert oraz wymuszone działanie – restart) o przekroczeniu zadanego czasu pracy bez restartu systemu operacyjnego.

22. Oprogramowanie musi zapewniać automatyczny import drzewiastej struktury organizacyjnej zamawiającego (bez ograniczeń ilości zagnieżdżeń z kontenera Active Directory/OpenLDAP), kont użytkowników i komputerów z zachowaniem ich oryginalnego położenia wg. OU.

23. Oprogramowanie musi zapewniać w obrębie synchronizacji z Active Directory/OpenLDAP tworzenie listy filtrów zawężających węzły danych wraz z możliwością wskazania docelowej gałęzi struktury organizacyjnej lub lokalizacyjnej Zamawiającego.

24. Oprogramowanie musi posiadać kreator powiązań (mapowanie atrybutów) dowolnych atrybutów obiektów z usługi katalogowej do wskazanych atrybutów zasobów systemowych.

25. Oprogramowanie musi umożliwiać współpracę z nieograniczoną ilością kontrolerów domen z zachowaniem podległej struktury drzewiastej.

26. Oprogramowanie musi umożliwiać automatyczny import informacji dotyczących przynależności użytkowników oraz stanowisk komputerowych do grup struktury katalogowej.

27. Oprogramowanie musi posiadać raport przedstawiający informacje nt. grup struktury katalogowej wraz przynależącymi do nich użytkownikami.

28. Oprogramowanie musi umożliwiać tworzenie dynamicznych grup stanowisk w oparciu o kreator zawierający filtry (AND, OR) w zakresie min. wersja OS, nazwa oraz wersja wybranej aplikacji, RAM, CPU, HDD, jednostka organizacyjna, jednostka lokalizacyjna, architektura (x32, x64), zainstalowane oprogramowanie, wersja oprogramowania, lista usług systemowych, producent oraz model komputera, poziom uprawnień użytkownika, zainstalowana usługa systemowa, ostatnie uruchomienie systemu, obecność pliku EXE na dysku, predefiniowane atrybuty komputera (np. dostawca, numer faktury, data zakupu).

29. Oprogramowanie musi umożliwiać prezentację widoku zarządzanych stanowisk komputerowych w postaci listy stanowisk, drzewiastej struktury wg jednostek organizacyjnych, jednostek lokalizacyjnych, struktury Active Directory, struktury sieciowej (pule IP) oraz grup dynamicznych.

30. Oprogramowanie musi umożliwiać dynamiczne zawężanie wyników wyszukiwania ww. widoków na podstawie prezentowanych w nich atrybutów.

31. Oprogramowanie musi umożliwiać graficzną prezentację aktualnego stanu aktywności agenta (online/offline) z dokładnością do 1 minuty.

32. Oprogramowanie musi umożliwiać zapisywanie w bazie danych informacji o uruchomieniu i wyłączeniu komputera oraz zalogowaniu i wylogowaniu użytkownika.

33. Oprogramowanie musi umożliwiać wydruk kartoteki sprzętowej stanowiska komputerowego.

34. Oprogramowanie musi umożliwiać samodzielną edycję wyglądu kartoteki sprzętowej, protokołów przekazania oraz zwrotu zasobów za pomocą graficznego kreatora wyglądu.

35. Oprogramowanie musi umożliwiać zapisywanie edytowanych szablonów (min. kartoteka sprzętowa, protokoły przekazania/zwrotu zasobów) w kontekście zalogowanego operatora konsoli zarządzającej.

36. Oprogramowanie musi umożliwiać projektowanie, generowanie oraz wydruk etykiet inwentaryzacyjnych w zakresie: model, nr inwentaryzacyjny, data zakupu, jednostka, wraz z obsługą kodów kreskowych w standardzie EAN128 oraz PDF417

37. Oprogramowanie musi umożliwiać okresową automatyczną inwentaryzację parametrów sprzętowych stanowiska: HDD, RAM, CPU, karta sieciowa, system operacyjny, karta graficzna itp.

38. Oprogramowanie Agenta musi umożliwiać audyt off-line, poprzez uruchomienie skanera (z GUI) bez konieczności instalacji, oraz zapis wyników do pliku w postaci zaszyfrowanej.

39. Oprogramowanie musi umożliwiać analizę sprzętową:

a. płyty głównej w zakresie model, producent, nr. Seryjny,

b. CPU w zakresie nazwy, modelu, producenta, częstotliwości,

c. HDD w zakresie numeru seryjnego dysku, numeru seryjnego partycji, rozmiaru pamięci,

d. RAM w zakresie wielkości pamięci,

e. karty sieciowej w zakresie model, adres IP, adres MAC,

f. karty graficznej w zakresie model.

40. Oprogramowanie musi umożliwiać odczyt informacji dotyczących systemu operacyjnego w zakresie nazwy, wersji, daty instalacji, zainstalowanych poprawek, dostępnych kluczy licencyjnych, produkt ID.

41. Oprogramowanie musi umożliwiać odczyt informacji sieciowych w zakresie adresu IO, adresu MAC, nazwy sieciowej.

42. Oprogramowanie musi umożliwiać odczyt informacji sprzętowych z BIOS w zakresie nazwy BIOS, daty, producenta.

43. Oprogramowanie musi umożliwiać przegląd historii zmian parametrów sprzętowych komputerowych.

44. Oprogramowanie musi umożliwiać globalny przegląd stanowisk komputerowych pod względem parametrów sprzętowo-systemowych.

45. Oprogramowanie musi zawierać raport stanowisk komputerowych posiadających co najmniej jedno konto z uprawnieniami administratora.

46. Oprogramowanie musi umożliwiać odczyt urządzeń podłączonych do stanowiska komputerowego przez interfejs USB, z możliwością odczytania nazwy urządzenia, producenta, modelu oraz numeru seryjnego (o ile urządzenie dostarcza ww. informacji)

47. Oprogramowanie musi umożliwiać globalną analizę urządzeń podłączonych do stanowisk komputerowych przez interfejs USB

48. Oprogramowanie musi umożliwiać integrację z zewnętrzną usługą Dell API w celu automatycznego odczytania informacji na temat okresu gwarancji stanowiska komputerowego na podstawie odczytanego przez agenta identyfikatora (ServiceTag)

49. Oprogramowanie musi umożliwiać okresowe próbkowanie obciążenia procesora oraz zajętości pamięci RAM z możliwością zapisu odczytanych wyników do bazy w celu późniejszej analizy (historia obciążenia komputera).

50. Oprogramowanie musi umożliwiać automatyczną inwentaryzację zainstalowanego na komputerach oprogramowania.

51. Oprogramowanie musi umożliwiać globalny przegląd wszystkich programów zainstalowanych na komputerach.

52. Oprogramowanie musi umożliwiać tworzenie zestawień zainstalowanych typów programów (freeware, shareware itp.).

53. Oprogramowanie musi umożliwiać tworzenie wykazów z zainstalowanym, dowolnie wybranym programem.

54. Oprogramowanie musi umożliwiać tworzenie zestawień zainstalowanych systemów operacyjnych na komputerach.

55. Oprogramowanie musi umożliwiać tworzenie wykazów stanowisk z brakiem zainstalowanego, dowolnie wybranego, programu.

56. Oprogramowanie musi posiadać wbudowany mechanizm umożliwiający, poprzez GUI konsoli, zdalną grupową dezinstalację oprogramowania np. pakietów MS Office.

57. Oprogramowanie musi umożliwiać oznaczanie kolorem aplikacji zabronionych oraz zgodnych ze standardem wraz z możliwością raportowania wg w/w klasyfikacji.

58. Oprogramowanie musi umożliwiać zablokowanie na stacji roboczej wybranych procesów celem uniemożliwienia ich uruchomienia przez użytkownika.

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

60. Oprogramowanie musi posiadać wbudowaną bazę sygnatur aplikacji (produktów) wraz z możliwością automatycznej aktualizacji wzorców ze strony Producenta oprogramowania

61. Oprogramowanie musi umożliwiać zdefiniowanie własnych sygnatur aplikacji (produktów) wykorzystywanych

w procesie automatycznego audytu licencji (rozliczenie ilościowe).

62. Oprogramowanie musi umożliwiać wykonanie audytu licencji tj. systemowego porównania zidentyfikowanego na stanowiskach komputerowych oprogramowania (produktów) z zakupionymi licencjami wprowadzonymi do systemu jako odpowiednie obiekty. Mechanizm audytu musi umożliwiać rozliczenie licencji z wykorzystaniem mechanizmów downgrade, upgrade.

63. Oprogramowanie musi umożliwiać zapis historii wykonywanych audytów licencji.

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

65. Oprogramowanie musi umożliwiać interakcję administratora z użytkownikiem, polegającą na podłączeniu do stanowiska (przejęcie pulpitu) administratora bez konieczności uprzedniego wylogowania użytkownika. Funkcjonalność zdalnego pulpit nie może wymagać instalacji aplikacji firm trzecich, wymagane jest obsłużenie przejęcia zdalnego pulpitu przez mechanizm wbudowany w agencie (ten sam proces systemowy).

66. Oprogramowanie musi umożliwiać wybór monitora, którego ekran ma zostać przejęty podczas połączenia zdalnego. Podczas aktywnego połączenia zdalnego, użytkownik jest informowany o trwaniu sesji zdalnej poprzez wyświetlanie na aktywnym monitorze kontrastowego obramowania ekranu.

67. Oprogramowanie musi umożliwiać zdalne zarządzanie (bez użycia RDP/VNC itp.) lokalnymi kontami użytkowników w zakresie (tworzenie, usuwanie, edycja, zmiana hasła oraz typ konta).

68. Oprogramowanie musi umożliwiać wysyłanie polecenia Wake-on LAN.

69. Oprogramowanie musi umożliwiać zdalną dwukierunkową linię poleceń.

70. Oprogramowanie musi umożliwiać przesyłanie plików/katalogów od zdalnego użytkownika do administratora i/lub od administratora do zdalnego użytkownika bez względu na lokalizację sieciową komputera (LAN, WAN, Internet).

71. Oprogramowanie musi umożliwiać konfigurację przez administratora parametrów połączenia z użytkownikiem w zakresie: ilość kolorów, ilość klatek/sekundę, skalowanie okna użytkownika, jeżeli jest ono większe niż rozdzielczość stacji administratora.

72. Oprogramowanie musi umożliwiać wybór aktywnych sesji terminalowych, do których chcemy się podłączyć.

73. Oprogramowanie musi umożliwiać zbiorczy podgląd zdalnych pulpitów stacji.

74. Oprogramowanie musi posiadać zarządzanie technologią iAMT, vPro w zakresie uwzględniającym min.: Serial Over Lan (SOL), IDE Redirection (IDER), Hardware KVM, Assets.

75. Oprogramowanie musi zapewniać zdalną konfigurację technologii iAMT w trybie Client Control Configuration Mode.

76. Oprogramowanie musi umożliwiać zarządzanie stacjami komputerowymi poza siecią LAN/WAN, wymagane jest tylko dowolne połączenie internetowe

77. Oprogramowanie musi umożliwiać zdalne wykonywanie zapytań WQL

78. Oprogramowanie musi umożliwiać zdalny odczyt oraz modyfikację rejestru Windows

79. Oprogramowanie musi umożliwiać pełne wykorzystanie funkcji zawartych w sekcji zdalne zarządzanie dla stacji posiadających dowolne połączenie do sieci INTERNET bez konieczności zestawiania połączenia VPN

80. Oprogramowanie musi umożliwiać przejęcie pulpitu zdalnego z poziomu konsoli zarządzającej znajdującej się poza siecią LAN organizacji poprzez połącznie konsoli ze wskazanym serwerem aplikacji.

81. Oprogramowanie musi umożliwiać prowadzenie w czasie rzeczywistym dwukierunkowej komunikacji tekstowej (chat) pomiędzy użytkownikiem a administratorem.

82. Oprogramowanie musi umożliwiać zdalną instalację pakietów \*.msi, plików \*.cmd, \*.bat, \*.reg, \*.ps1 poprzez utworzenie zadań dystrybucji aplikacji oraz wskazanie docelowych komputerów lub grup komputerów za pomocą dedykowanego GUI użytkownika. Zadanie dystrybucji musi umożliwiać określenie okresu aktywności, godziny rozpoczęcia oraz przedstawiać status instalacji na wybranych stanowiskach.

83. Oprogramowanie musi umożliwiać tworzenie zadań dystrybucji polegające na jednorazowym uruchomieniu wybranego szablonu akcji na wybranych stanowiskach komputerowych.

84. Oprogramowanie musi umożliwiać tworzenie polis uruchamianych cyklicznie na wybranych stanowiskach komputerowych wg aktualnej przynależności do struktury organizacyjnej, lokalizacyjnej lub wybranych grup dynamicznych.

85. Oprogramowanie musi umożliwiać tworzenie dystrybucji zadań oraz polis dla wybranych stanowisk komputerowych poprzez interaktywny kreator (krok po kroku). Wybór odbiorców musi uwzględniać listę stanowisk, strukturę organizacyjną, strukturę lokalizacyjną oraz dynamiczne grupy stanowisk.

86. Oprogramowanie musi umożliwiać globalną dystrybucję plików oraz folderów do wskazanych lokalizacji do wybranych stanowisk komputerowych wg przynależności do struktury organizacyjnej, lokalizacyjnej lub grupy dynamicznej wraz z automatycznym (polisa) odtworzeniem brakujących danych w przypadku wykrycia niespójności.

87. Oprogramowanie musi umożliwiać szyfrowanie plików źródłowych dla zadań instalacji.

88. Oprogramowanie musi umożliwiać globalny przegląd postępu wykonania wybranych zadań oraz polis wraz z odczytem standardowego wyjścia (stdout) oraz standardowego wyjścia błędów (stderr).

89. Oprogramowanie musi umożliwiać tworzenie własnych szablonów akcji zawierających zdefiniowaną listę akcji pozwalających na warunkowe uruchamianie akcji zależnych (oczekiwanie na zakończenie akcji, praca w tle).

90. Oprogramowanie musi umożliwiać konfigurację typów akcji co najmniej w zakresie: dystrybucja i uruchomienie plików wsadowego BAT, dystrybucja plików rejestru REG, dystrybucja i instalacja pakietu MSI, dystrybucja i instalacja poprawki MSP, dystrybucja i uruchomienie aplikacji EXE, dystrybucja i uruchomienie skryptu PowerShell, dystrybucja plików i folderów, uruchomienie/wyłączenie/restart usługi systemowej, zakończenie procesu systemowego, wywołanie polecenia CMD.

91. Oprogramowanie musi umożliwiać konfigurowanie dedykowanych parametrów dla każdej z ww. akcji.

92. Oprogramowanie musi umożliwiać uruchomienie na prawach administracyjnych pliku instalacyjnego EXE (z GUI) w sesji użytkownika z ograniczonymi uprawnieniami do instalacji aplikacji. Proces instalacji jest manualnie kontynuowany przez użytkownika.

93. Oprogramowanie musi umożliwiać ograniczenie zakresu działania zadania, polisy oraz zawężenie wszelkich raportów systemowych do stanowisk spełniających kryteria wybranej dynamicznej grupy stanowisk.

94. Oprogramowanie w zakresie automatyzacji musi realizować m.in. następujące przypadki użycia z wykorzystaniem mechanizmu grup dynamicznych dla zadań oraz polis:

a. Automatyczną instalacji aplikacji na komputerach spełniających warunki: stanowiska z Windows 10 z pamięcią RAM>4GB i zainstalowaną wybraną aplikacją w wersji mniejszej (np. 7.0)

b. Automatyczne odinstalowanie aplikacji na komputerach spełniających warunki: stanowiska z Windows 7 gdzie producentem komputera jest np. Dell i zainstalowaną wybraną aplikacją w wersji większej niż (np. 8.0)

Dystrybucję plików oraz folderów (ze wskazaną zawartością np. dokumenty, skróty do aplikacji) na pulpity stanowisk komputerowych spełniających warunki: stanowiska z Windows 10 z brakiem zainstalowanej wybranej aplikacji oraz nie posiadające konta użytkownika z prawami administracyjnymi

c. Uruchomienia wybranego skryptu PowerShell dla komputerów spełniających warunki: stanowiska z Windows 10 w architekturze 32 bitowej, zainstalowaną aplikacją X w wersji większej niż (np. 6.0) i brakiem zainstalowanej aplikacji Y.

d. Uruchomienia wybranych szablonów akcji w przypadku wykrycia zmiany jednostki organizacyjnej stanowiska komputerowego.

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

95. Oprogramowanie musi umożliwić instalację oprogramowania z plików exe, które nie posiadają instalacji w trybie cichym poprzez automatyzację procesu manualnej instalacji (nagrywanie makr w zakresie wyborów typu zaznaczenie checkbox, wybór pozycji z listy, kliknięcie przycisku, wpisanie parametru/ścieżki itp.)

96. Oprogramowanie musi posiadać repozytorium szablonów makr automatyzacji do późniejszego wykorzystania podczas procesów instalacji

97. Oprogramowanie musi zawierać funkcję testowania nagranych makr z poziomu interfejsu użytkownika

98. Oprogramowanie musi wznawiać instalację, w przypadku przerwania procesu instalacji (np. z powodu wyłączenia komputera)

99. Nagrywanie makr musi być realizowane przez wybranie/wskazanie elementu okna, na którym ma zostać wykonana akcja (np. kliknięcie, wprowadzenie tekstu, zaznaczenie)

100. Oprogramowanie musi umożliwiać wysyłanie komunikatów (Windows Notification) do wskazanych stanowisk komputerowych (wybór manualny, wg struktury organizacyjnej, lokalizacyjnej lub grupy dynamicznej)

101. Oprogramowanie musi umożliwiać wysyłanie komunikatów przed każdą zdefiniowaną akcją automatyzacji (np.: przed rozpoczęciem instalacji pakietu MSI, przed dystrybucją plików, przed uruchomieniem skryptu PowerShell)

102. Oprogramowanie musi umożliwiać automatyzację procesu konfiguracji dowolnej aplikacji Windows w celu odtworzenia zapamiętanych akcji (makr) dla wskazanych stanowisk komputerowych.

103. Oprogramowanie musi umożliwiać tworzenie dowolnej ilości automatycznych zadań w zakresie archiwizacji danych – globalnie z poziomu głównej konsoli zarządzającej.

104. Oprogramowanie musi umożliwiać globalną zmianę parametrów zadań archiwizacji (ilość archiwów, kompresja, okres, zakres).

105. Oprogramowanie musi umożliwiać definiowanie rozszerzeń plików, które mają być pomijane podczas procesu archiwizacji oraz rozszerzeń plików np. \*.doc, które mają być archiwizowane.

106. Oprogramowanie Agenta musi umożliwiać kopię całościową danych oraz przesyłanie plików z archiwizacji na wskazany serwer FTP.

107. Mechanizm archiwizacji danych musi być realizowany przez Agenta systemu bez udziału zdalnych sesji (typu zdalny pulpit, wywoływanie skryptów)

108. Oprogramowanie musi umożliwiać definiowanie cyklu archiwizacji.

109. Oprogramowanie musi umożliwiać automatyczne usuwanie starszych plików kopii całościowej, definiowanie globalnego zadania archiwizacji.

110. Oprogramowanie musi umożliwiać zapisywanie w bazie danych informacji o kopiowaniu z/do urządzeń zewnętrznych typu: Pendrive USB, dysk zewnętrzny.

111. Oprogramowanie musi posiadać raport w zakresie rejestracji informacji na temat użytkownika, który kopiował i/lub uruchamiał napęd, kiedy miało miejsce zdarzenie i jakie dokumenty zostały skopiowane.

112. Oprogramowanie musi umożliwiać blokadę oraz autoryzację wybranych urządzeń USB w obrębie klasy USBStorage.

113. Oprogramowanie musi umożliwiać włączenie trybu ReadOnly dla klasy USBStorage

114. Oprogramowanie musi umożliwiać całkowitą blokadę klasy FDD/CD/DVD

115. Oprogramowanie musi umożliwiać zestawienie najpopularniejszych adresów (jakie stanowiska je wywoływały, kiedy) z możliwością zapisu całego adresu lub tylko głównej strony.

116. Oprogramowanie umożliwia zestawienie najaktywniejszych stanowisk (pod kątem WWW), jakie adresy odwiedzały, kiedy, wszystkie zestawienia do poziomu: jednostka organizacyjna, stanowisko, zalogowany użytkownik.

117. Oprogramowanie musi umożliwiać analizę uruchamianych aplikacji (aktywność stanowisk wg aplikacji oraz wykorzystanie zainstalowanych aplikacji wg stanowisk).

118. Oprogramowanie musi umożliwiać analizę efektywności pracy użytkowników na poszczególnych aplikacjach

119. Oprogramowanie musi umożliwiać blokadę stron www (biała i czarna lista adresów, blokada pełna lub selektywna) z możliwością automatycznego zamykania przeglądarki lub konkretnej karty przeglądarki (w przypadku wykrycia adresu zabronionego).

120. Oprogramowanie musi umożliwiać tworzenie statystyk aktywności stron WWW oraz aktywności stanowisk.

121. Oprogramowanie musi umożliwiać podział stron na dozwolone i zabronione.

122. Oprogramowanie musi umożliwiać wydruki tabelaryczne oraz graficzne (wykresy aktywności).

123. Oprogramowanie musi umożliwiać okresowe tworzenie zrzutu ekranu użytkownika z możliwością przesłania go na serwer.

124. Oprogramowanie musi umożliwiać rozróżnienie stanów monitorowanego komputera w szczególności stan aktywności (focus okna), hibernacji, uśpienia oraz wylogowania

125. Oprogramowanie musi umożliwiać odczyt aktywności użytkownika w czasie rzeczywistym w zakresie min. tytuł okna, adres www przeglądanej strony z dokładnością do 1 sekundy.

126. Oprogramowanie musi umożliwiać analizę aktywności myszy oraz klawiatury dla poszczególnych monitorowanych aplikacji oraz stron internetowych (ilość kliknięć).

127. Oprogramowanie musi umożliwiać monitorowanie wszystkich prac drukowania generowanych na urządzeniach sieciowych udostępnionych przez centralny serwer wydruków i udostępnionych lokalnie przez port TCP/IP

128. Oprogramowanie musi umożliwiać monitorowanie wszystkich prac drukowania generowanych na urządzeniach lokalnych udostępnionych przez port LPT, USB. Monitorowanie tych wydruków musi odbywać się poprzez agenta aplikacji zainstalowanego na stacji roboczej będącej serwerem wydruków dla drukarki lokalnej.

129. Oprogramowanie po zainstalowaniu musi przesyłać do serwera aplikacji następujące informacje: nazwa stacji roboczej, nazwa zainstalowanego sterownika drukarki, nazwa portu z jakiego dany sterownik korzysta, opis sterownika drukarki, format drukowanych stron oraz nazwę drukowanego dokumentu.

130. Oprogramowanie musi posiadać możliwość definicji kosztów wydruku dla poszczególnych urządzeń drukujących (podział kosztu na mono/kolor).

131. Oprogramowanie musi umożliwiać okresowe skanowanie sieci LAN (wg. zadanych kryteriów, na wybranych serwerach lokalnych) z wykorzystaniem protokołu SNMP, celem prezentacji aktywnych urządzeń IP w zakresie co najmniej komputery, drukarki, routery, smartphony

132. Oprogramowanie musi umożliwiać monitorowanie poprzez wykorzystanie protokołu SNMP stanu drukarek tj. poziomy tonerów, liczba wydrukowanych stron oraz informować błędach takich jak brak papieru, zacięcie papieru.

133. Oprogramowanie musi umożliwiać wizualizację ruchu sieciowego na poszczególnych portach urządzeń sieciowych wraz z wizualizacją w postaci mapy sieci dla wskazanego urządzenia typu switch, router.

134. Oprogramowanie musi umożliwiać z zdalną instalację agenta systemu z poziomu wykrytej struktury sieciowej z wykorzystaniem poświadczeń administracyjnych, w tym również stanowisk poza usługą katalogową.

135. Oprogramowanie musi umożliwiać monitorowanie stanu dowolnej usługi sieciowej TCP.

136. Oprogramowanie musi umożliwiać monitorowanie dowolnego licznika SNMP(v1/2/3) urządzenia.

137. Oprogramowanie musi umożliwiać monitorowanie stanu dowolnego urządzenia sieciowego poprzez odpytywanie typu PING.

138. Oprogramowanie musi umożliwiać tworzenie konfigurowalnych zdarzeń sieciowych powodujących wysyłanie komunikatów informacyjnych i/lub ostrzegawczych poprzez SMS i/lub Email.

139. Zamawiający wymaga udostępnienia oprogramowania spełniającego wymagania w licencji wieczystej.

140. W okresie trwania umowy wymagany jest dostęp do nowych wersji systemu oraz wsparcia technicznego producenta.

141. Obsługa serwisowa musi być realizowana przez Producenta oprogramowania, w dni robocze w godzinach 8-16 w języku polskim, zgodnie z poniższymi parametrami:

142. Dostarczone licencje na oprogramowanie muszą objąć co najmniej 35 stanowisk komputerowych z systemem klasy Microsoft Windows. Licencje nie mogą mieć ograniczeń ilościowych dotyczących liczby obsługiwanych innych zasobów (np. drukarki, skanery, monitory itp). Ponadto musi posiadać co najmniej 1 licencji dostępowych do konsoli zarządzającej.

143. Zamawiający wymaga wsparcia dedykowanego konsultanta technicznego w wymiarze 50 godzin dla okresu trwania umowy.

144. W przypadku wątpliwości zamawiający zastrzega sobie prawo (w przeciągu do 7 dni od terminu otwarcia ofert) do wezwania wykonawcy do prezentacji zaoferowanego rozwiązania celem weryfikacji zgodności z wymaganiami stawianymi przez zamawiającego w niniejszym postępowaniu.

145. Zamawiający wymaga od wykonawcy, aby w terminie 90 dni od podpisania umowy przeprowadził wdrożenie systemu zdalnie (wymagana co najmniej 2 sesji – 2 godzin każda)

146. Zamawiający wymaga od wykonawcy, aby w terminie 30 dni od zakończenia prac wdrożeniowych przeprowadził szkolenie z obsługi systemu w siedzibie zamawiającego/zdalnie (wymagana co najmniej 2 sesje – 2 godzinne)

**IX. Przełącznik sieciowy – 2 szt.**

Przedmiotem zamówienia jest przełącznik sieciowy z 48 portami klasy Enterprise.

Wymagania:

1. Porty i interfejsy:

a. Co najmniej 48 portów obsługujących standard 10/100/1000BASE-T, zapewniających automatyczne negocjowanie prędkości, z czego min. 24 porty muszą obsługiwać PoE+ (802.3af/at) z łącznym budżetem mocy min. 370W

b. Minimum 4 porty uplink obsługujące standard 10 GbE SFP+ dla szybkiej transmisji danych,

c. 1 port serial RJ45 do konsoli.

2. Wydajność i przepustowość:

a. Przepustowość przełączania na poziomie co najmniej 176 Gbps,

b. Prędkość przesyłania pakietów (packet forwarding rate) nie mniejsza niż 260 Mpps.

c. Obsługa minimum 32 tys. adresów MAC,

d. Bufor na pakiety o wielkości min. 2MB,

e. Pamięć RAM min. 512MB DDR3,

f. Pamięć flash min. 64MB,

g. Obsługa agregacji łączy (LACP) dla zwiększenia wydajności i redundancji.

3. Zarządzanie i konfiguracja:

a. Możliwość zarządzania przez interfejs CLI, GUI oraz protokoły SNMP i REST API,

b. Obsługa min. 4000 VLAN (IEEE 802.1Q) i funkcji QoS umożliwiających priorytetyzację ruchu sieciowego,

c. Funkcje monitorowania i zabezpieczeń, w tym kontrola dostępu na poziomie portów (802.1X), wykrywanie pętli oraz ochrona przed atakami typu DoS.

4. Bezpieczeństwo i funkcje sieciowe:

a. Obsługa min. 640 list kontroli dostępu (ACL) dla zarządzania ruchem sieciowym,

b. Możliwość segmentacji sieci przy użyciu technologii VLAN oraz dynamicznego przypisywania VLAN-ów.

c. Zabezpieczenia warstwy 2, w tym ochrona przed spoofingiem ARP oraz filtrowanie MAC.

5. Zasilanie i warunki eksploatacyjne:

a. Wbudowany zasilacz w standardzie AC 100–240 V, 50/60 Hz,

b. Maksymalny pobór mocy poniżej 480W,

c. Obudowa 1U RACK 19" o głębokości poniżej 32 cm,

d. Zakres temperatury pracy od 0°C do co najmniej 45°C.

6. Dodatkowe wymagania:

a. Wsparcie serwisowe producenta dla aktualizacji oprogramowania w celu zapewnienia zgodności z nowymi standardami bezpieczeństwa i wydajności przez okres minimum rok,

b. Możliwość pracy w trybie standalone oraz w integracji z centralnym systemem zarządzania siecią.

**X. Punkty bezprzewodowe – 1 kpl.**

Przedmiotem zamówienia jest dostawa, instalacja oraz konfiguracja kontrolera oraz 4 szt. bezprzewodowych punktów dostępowych.

Wymagania:

1. Kontroler sprzętowy sieci bezprzewodowej WiFi:

a. Kontroler musi umożliwiać zarządzanie punktami dostępowymi w liczbie min 100.

b. Kontroler musi mieć możliwość zarządzania zarówno urządzeniami odpowiadającymi za segment bezprzewodowy sieci (punkty dostępowe) jak i urządzeniami tworzącymi warstwę dostępową i szkielet sieci (przełączniki)

c. Urządzenie musi być wyposażone w min. 2 porty RJ45 o prędkości 10/100Mb/s

d. Urządzenie musi być wyposażone w port USB umożliwiający podłączenie zewnętrznego nośnika danych

e. Urządzenie musi posiadać następujące certyfikaty: CE, RoHS

f. Dopuszczana temperatura pracy urządzenia musi zawierać się w przedziale od 0 do 40 stopni Celsjusza

g. Urządzenie musi umożliwiać automatyczne wykrywanie wszystkich urządzeń w sieci lokalnej kompatybilnych z Kontrolerem

h. Urządzenie musi zapewniać możliwość zdalnego zarządzania siecią w danej lokalizacji wykorzystując chmurę lub inny mechanizm pozwalający na dostęp do kontrolera z dowolnego miejsca

i. ACL (listy kontroli dostępu) zarówno dla użytkowników łączących się do sieci przewodowo jak i bezprzewodowo

j. W zakresie konfiguracji sieci WiFi urządzenie musi umożliwiać konfigurację następujących funkcji:

i. Multi SSID

ii. Sieć dla Gości (odizolowanie klientów w tej sieci od innych klientów lokalnych bez wykorzystania VLAN)

iii. Powiązanie SSID do VLAN

iv. Filtrowanie adresów MAC (tryby blacklist/whitelist)

v. Kanał transmisji/moc nadawania konkretnych AP

vi. Równoważenie obciążenia punktów dostępowych

vii. Sterowanie pasmem

viii. Ograniczenie prędkości transmisji

ix. Tworzenie harmonogramu sieci WiFi oraz resetu urządzeń

x. QoS

xi. Harmonogramowanie sieci bezprzewodowej oraz restartu urządzenia

2. Zestaw 4 szt. punktów dostępowych sieci WiFi:

a. Urządzenia muszą być wyposażone w min. 1 port RJ45 pracujące z prędkością 2.5Gb/s

b. Jeden z portów musi być portem PoE PD umożliwiającym zasilenie urządzenia przez skrętkę zgodnie z jednym ze standardów: 802.3at

c. Urządzenia muszą być wyposażone w gniazdo umożliwiające zasilanie urządzenia bezpośrednio z wykorzystaniem zewnętrznego zasilacza

d. Urządzenia muszą być wyposażone w przycisk przywracania ustawień fabrycznych

e. Urządzenia muszą być wyposażone w min 3 anteny wewnętrzne dookólne o zysku min 4dBi dla sieci 2,4GHz, min. 5dBi dla sieci 5GHz oraz min. 5dBi dla sieci 6GHz

f. Urządzenia muszą wspierać standardy IEEE 802.11a/b/g/n/ac/ax/be oraz częstotliwości pracy 2,4GHz, 5GHz oraz 6GHz

g. Łączna prędkość modułów radiowych musi wynosić min. 9000Mbps

h. Maksymalny pobór mocy urządzenia nie może być większy niż 25W

i. Urządzenia muszą umożliwiać montaż na ścianie lub suficie

j. Urządzenia muszą pracować zarówno jako urządzenie typu stand-alone lub w trybie podłączonym do kontrolera sieci bezprzewodowej

k. Kontroler sieci bezprzewodowej realizowany musi być jako kontroler sprzętowy – oddzielne urządzenie

l. Urządzenia muszą posiadać funkcjonalność tworzenia wielu sieci WiFi – min. 24 SSID

m. Urządzenia muszą posiadać funkcjonalność: wyłącznik sieci bezprzewodowej, automatyczny wybór kanału, kontrola mocy transmisji, QoS (WMM), sterowanie pasmem, równoważenie obciążenia pasma, kontrola przepustowości, harmonogram resetu oraz harmonogram sieci bezprzewodowej.

n. Urządzenia muszą posiadać możliwość utworzenia strony powitalnej

o. Urządzenia muszą posiadać możliwość mapowania SSID do VLAN oraz tworzenia sieci dla gości

p. Urządzenia muszą być zarządzane z poziomu przeglądarki internetowej, oraz obsługiwać zarządzanie poprzez HTTPS

r. Urządzenia muszą posiadać obsługę SNMP v1/v2c,v3

s. Urządzenia muszą posiadać certyfikat CE oraz RoHS

t. W zestawie z urządzeniami powinien być dostarczony zestaw montażowy

u. Dopuszczalna temperatura pracy powinna zawierać się w przedziale od 0 do 40 stopni Celsjusza.

3. Urządzenia muszą posiadać certyfikację CE

4. Gwarancja na urządzenia musi wynosić min. 36 miesięcy.

5. Wszystkie dostarczone urządzenia muszą pochodzić z polskiego autoryzowanego kanału dystrybucyjnego producenta. Na wezwanie Zamawiającego Wykonawca musi dostarczyć oświadczenie producenta oferowanych urządzeń, potwierdzające pochodzenie urządzeń i oprogramowania z oficjalnego kanału dystrybucyjnego producenta.

6. Zakres prac wdrożeniowych:

a. Opracowanie planu wdrożenia.

b. Wdrożenie i konfiguracja:

i. Instalacja urządzeń we wskazanych miejscach.

ii. Konfiguracja urządzeń zgodnie z wymaganiami zamawiającego.

iii. Integracja z istniejącymi systemami IT zamawiającego.

c. Testy akceptacyjne:

i. Przeprowadzenie testów funkcjonalnych i wydajnościowych wymaganych przez Zamawiającego potwierdzających zadeklarowane funkcjonalności. Wynik negatywny jakiejkolwiek funkcjonalności lub testu pozwala Zamawiającemu odrzucić proponowaną ofertę i odstąpić od umowy bez podania przyczyny.

ii. Weryfikacja poprawności działania urządzeń.

**XI. Agregat – 1 szt.**

Przedmiotem zamówienia jest dostawa, instalacja oraz konfiguracja 1 szt. agregatu wraz z Systemem Załączania Rezerwy (SZR).

Wymagania:

1. Agregat musi być wykonany zgodnie z obowiązującymi normami i standardami:

a. 2006/42/WE Dyrektywa Maszynowa

b. Kompatybilność elektromagnetyczna 2014/30/UE.

c. 2014/35/UE sprzętu elektrycznego przewidzianego do stosowania w określonych granicach napięcia

d. PN-EN ISO 8528-13:2016-07

e. PN- EN ISO 3744:2011

f. ISO 8528-1:20052000/14/WE, 2005/88/WE – Dyrektywa Hałasowa

g. Klasa wykonania minimum G2.

2. Wymagane jest aby agregat pochodził z seryjnej i bieżącej produkcji.

3. Agregat musi być w wersji obudowanej o poniższych parametrach:

a. Wymagana moc znamionowa agregatu – 25 kVA (20 kW).

b. Wymagana moc awaryjna agregatu nie mniej niż – 27 kVA (22 kW).

c. Napięcie – 400/230 V.

d. Częstotliwość – 50Hz.

e. Posiadać oznaczenie CE.

4. Agregat musi być w całości spreparowane przez jednego producenta posiadającego wdrożony system ISO 9001:2015.

5. Obudowa musi być dźwiękochłonna, wyciszona specjalną, niepalną pianką wygłuszającą, z czterema niezbędnymi drzwiami dostępowymi na dłuższych bokach.

6. Wylot spalin i gorącego powietrza poprzez górną połać obudowy.

7. Podejście kablowe umiejscowione na dłuższym boku po lewej stronie, bezpośrednio pod wyłącznikiem głównym agregatu, umożliwiające wprowadzenie okablowania bez wychodzenia kablami poza obrys agregatu.

8. Bardzo mocna konstrukcja z możliwością transportu wózkiem widłowym, dźwigiem, HDS – na pasach, widłach lub łańcuchach.

9. Rama dodatkowo izolowana od podłoża za pomocą stóp (stożków) gumowych przykręcanych do ramy.

10. Zewnętrzny przycisk zatrzymania awaryjnego.

11. Zaciski na listwie sterowniczej:

a. styk NC do podłączenia okablowania zewnętrznego stopu pożarowego

b. dla podłączenia okablowania potrzeb własnych agregatu.

c. dla podłączenia okablowania sterowania układem SZR.

12. Wysokowydajne amortyzatory drgań silnika i prądnicy.

13. Pojemnościowy czujnik poziomu paliwa z % wskazaniem na sterowniku

14. Alarm poziomu paliwa 15% (rezerwa)

15. Wyłączenie agregatu przy 5% paliwa (zabezpieczenie przed zapowietrzeniem)

16. Wymagany również korek spustowy zbiornika oraz co najmniej jeden niezależny, otwór w zbiorniku zaślepiony deklem na śrubach, umożliwiający montaż i podłączenie dodatkowej instalacji paliwowej.

17. Silnik diesla o mocy znamionowej PRP nie mniejszej niż – 23 kW.

18. Liczba i układ cylindrów – 4 L.

19. Wymagany typ wtrysku – bezpośredni.

20. Elektroniczna regulacja obrotów.

21. Emisja spalin - min. Stage II.

22. Podgrzewanie bloku – grzałka silnika kontrolowana przez sterownik agregatu.

23. Spalanie przy 75% obciążenia nie więcej niż – 4,5 l/h.

24. Spalanie przy 100% obciążenia nie więcej niż – 6,1 l/h.

25. Wlew paliwa - korek zamykany kluczykiem, wewnątrz obudowy.

26. Filtr powietrza suchy.

27. Silnik chłodzony glikolem.

28. Prędkość obrotowa – 1500 r.p.m.

29. Układ elektryczny 12V.

30. Akumulator 12V.

31. Automatyczna ładowarka buforowa akumulatora/ów 12V/5A w czasie czuwania.

32. Osłona elementów gorących oraz ruchomych.

33. Prądnica wyposażona w automatyczną regulację napięcia

34. Obudowa (wg IEC-34-5) - IP23.

35. Złącze – elastyczny dysk.

36. Klasa izolacji – H.

37. Wymagane wykonanie, gdzie stojan prądnicy jest nawinięty z poskokiem 2/3, ponieważ zapewnia to eliminację krotności trzeciej harmonicznej (3, 9, 15, itd.) napięcia wyjściowego. Poskok 2/3 minimalizuje indukowanie się nadmiernych prądów w obwodzie neutralnym.

38. Wytrzymałość zwarciowa prądnicy >300% obciążenia znamionowego.

39. Sterownik z pełną obsługą rozwiązań producenta, z komunikatami w języku polskim, pozwalający na kontrolę parametrów sieci i agregatu (napięć, prądów, mocy, częstotliwości, cos ɸ, napięcia ładowania akumulatora, ilość paliwa w zbiorniku, czasu pracy agregatu, parametrów silnika).

40. Panel sterownika wyposażony w tabliczkę z diodami sygnalizacyjnymi dla łatwej obsługi i szybkiej identyfikacji stanów pracy urządzenia. Wymagana jest identyfikacja alarmów dotyczących działania baterii, pracy alternatora, poziomu paliwa, ciśnienia oleju oraz dwa dodatkowe do zdefiniowania. Sterownik musi posiadać w tylnej ścianie wolne sloty do podłączenia dodatkowych modułów sygnalizacyjnych np. GSM, ETHERNET, styków/wyjść przekaźnikowych dla sygnałów bezpotencjałowych (do zdefiniowania przez użytkownika)

41. Szafa elektryczna/automatyki agregatu zbudowana na podzespołach renomowanych producentów elektryki i elektroniki, według norm i standardów.

42. Sterownik musi posiadać ekonomiczny kontroler agregatu gotowy do integracji BMS i monitorowania poprzez Internet

43. Cechy sterownika agregatu:

a. Obsługa na olej napędowy

b. Obsługa 400 Hz

c. Dziennik - 400 zdarzeń

d. Możliwość edycji wszystkich parametrów na panelu przednim

e. 3-poziomowe hasło konfiguracyjne

f. Graficzny wyświetlacz LCD 128x64

g. Języki do pobrania (domyślnie – polski)

h. Wyświetlanie przebiegów napięcia i prądów

i. Analiza harmonicznych

j. Wyjścia 16 A MCB i GCB

k. 8 konfigurowalnych wejść cyfrowych

l. Wejścia rozszerzalne do 40

m. 6 konfigurowalnych wyjść cyfrowych

n. Wyjścia z możliwością rozszerzenia do 38

o. 3 konfigurowalne wejścia analogowe

p. Zarówno CANBUS-J1939, jak i MPU

q. 3 konfigurowalne alarmy serwisowe

r. Tygodniowy harmonogram pracy

s. Ręczna „precyzyjna regulacja prędkości” w wybranych ECU

t. Automatyczne sterowanie pompą paliwa

u. Ochrona przed nadmierną mocą

v. Odwrotna ochrona zasilania

w. Zabezpieczenie przed przeciążeniem IDMT

x. Zrzut obciążenia, obciążenie zastępcze

y. Zarządzanie wieloma obciążeniami

z. Zabezpieczenie od asymetrii prądu

aa. Ochrona przed asymetrią napięcia

bb. Zegar czasu rzeczywistego z podtrzymaniem bateryjnym

cc. Kontrola prędkości biegu jałowego

dd. Ładowanie akumulatora włączone

ee. Wiele parametrów nominalnych

ff. Napęd Tactor i MCB

gg. 4 kwadrantowe liczniki mocy agregatu

hh. Liczniki zasilania sieciowego

ii. Wskazania poziomu paliwa

jj. Wyświetlacz diagnostyczny modemu

kk. Konfigurowalny przez USB, RS-485 i GPRS

ll. Darmowy program konfiguracyjny

mm. Gotowy do centralnego monitorowania

nn. Obsługa mobilnych agregatów prądotwórczych

oo. Łatwa aktualizacja oprogramowania sprzętowego USB

pp. Stopień ochrony IP65 ze standardową uszczelką

44. Pomiary:

a. Napięcia sieci i agregatu PN / PP

b. Częstotliwość sieci i agregatu

c. Prądy fazowe sieci i agregatu

d. Prądy neutralne sieci i agregatu

e. Sieć i agregat, faza i suma, kW, kVA, kVAr, pf

f. Prędkość silnika

g. Napięcie baterii

h. Temperatura silnika

i. Ciśnienie oleju

j. Zużycie paliwa (dla silników wyposażonych w ECU)

45. Komunikacja:

a. Port USB

b. RS-232 (2400-115200)

c. J1939-CANBUS

d. Centralny monitoring internetowy

e. Darmowe oprogramowanie na PC

f. Modbus RTU

46. Układ SZR typu RTSE na przełączniku z napędem silnikowym. Tryby sterowania:

a. Sterowanie automatyczne - W momencie zaniku napięcia sieci sterownik agregatu rozpoczyna odliczanie zaprogramowanej zwłoki czasowej. Po upłynięciu nastawionego czasu i utrzymującego się braku napięcia sieci sterownik przełącza się w pozycję „0” i wystawia sygnał START agregat, który rozpoczyna procedurę startu silnika napędzającego generator według zaprogramowanych w sterowniku agregatu parametrów (czas startowania i przerwa, ilość możliwych prób startowania itp.). Po pojawieniu się napięcia generatora, sterownik agregatu sprawdza jego parametry (wartość, częstotliwość) i gdy mieszczą się w dopuszczalnych granicach - przełącza układ w pozycję „II” przechodząc przez pozycję „0” i załącza kierunek zasilania z generatora. Tym samym napięcie generatora podane jest na odbiory.

b. Powrót napięcia - W momencie ponownego pojawienia się napięcia sieci i jego utrzymywania się przez odpowiedni czas, sterownik agregatu przełącza układ w pozycję „I” przechodząc przez pozycję „0” i załącza kierunek zasilania z sieci. Następnie utrzymuje jeszcze pracę silnika przez określony czas ok. 2 min, w celu umożliwienia wychłodzenia silnika bez obciążenia. Po upłynięciu tego czasu, sterownik agregatu wyłącza silnik napędzający generator i wraca do stanu wyjściowego tzn. do czuwania i monitorowania sieci.

c. Sterowanie ręczne mechaniczne - Przełącznik SZR można przestawiać przy pomocy dołączonej i wyjmowanej dźwigni/rączki.

47. W przypadku wyłączenia energii przez Zakład Energetyczny musi istnieć pewność, że napięcie z agregatu nie przedostanie się do sieci zasilającej. Podobnie rzecz ma się w drugim kierunku - napięcie z sieci nie może zostać podane na agregat. Jest to zapewnione przez niżej wymienione środki:

a. Budowa mechaniczna przełącznika – przełącznik źródła zasilania z napędem silnikowym 125A o trzech stabilnych pozycjach 1-0-2, składa się z dwóch niezależnych rozłączników 4-polowych izolacyjnych (tory główne) połączonych mechanicznie w sposób uniemożliwiający ich jednoczesne załączenie. Przełączenie źródeł odbywa się z przejściem przez pozycję 0.

b. Blokada elektryczna sterowania przełącznika – przełącznik posiada wewnętrzną blokadę uniemożliwiającą równoczesne wysterowanie dwóch pozycji przełącznika. Blokadę elektryczną zapewnia także układ mini SZR-a na zasilaniu i sterowaniu przełącznika zbudowany na ministycznikach z własną blokadą mechaniczną i elektryczną.

c. Blokada programowa – blokada ta uniemożliwia jednoczesne wysterowanie dwóch przekaźników zabudowanych wewnątrz sterownika agregatu podających sygnały do przełączania SZR-a.

48. Dane przełączeniowe:

a. I - czas trwania przerwy beznapięciowej przy przejściu z pozycji I do II bez postoju w poz.0 - tbn = 0,06s

b. II - czas trwania przerwy beznapięciowej z uwzględnieniem sterownika w trybie I-0-II i II-0-I (czas w poz.0 ustawiany w sterowniku) - tbn > 1,06s

c. III - czas przełączania w trybie I-0-II i II-0-I - tp > 1,18s

49. Na agregacie musi być zamontowana listwa odbioru mocy.

50. Wymagane jest:

a. aby dostawca posiadał umowę o współpracy z producentem agregatu w zakresie dostawy, uruchomienia i serwisowania dostarczonych maszyn i urządzeń dodatkowych.

b. aby producent agregatu posiadał w Polsce własny oddział, serwis oraz magazyn części zamiennych i materiałów eksploatacyjnych.

51. Przed dostarczeniem agregatu na obiekt należy wykonać próby FAT u producenta, w obecności komisji Zamawiającego i do dokumentacji powykonawczej załączyć stosowny protokół.

52. Gwarancja minimum 24 miesiące.

53. Zakres prac wdrożeniowych:

a. Opracowanie planu wdrożenia.

b. Pierwsze uruchomienie oraz konfiguracja agregatu i oprogramowania zgodnie z wymaganiami Zamawiającego. Integracja z istniejącymi systemami IT zamawiającego.

c. Przeprowadzenie testów funkcjonalnych i wydajnościowych wymaganych przez Zamawiającego potwierdzających zadeklarowane funkcjonalności. Wynik negatywny jakiejkolwiek funkcjonalności lub testu pozwala Zamawiającemu odrzucić proponowaną ofertę i odstąpić od umowy bez podania przyczyny.

d. Weryfikacja poprawności działania agregatu oraz oprogramowania

e. Szkolenie pracownika Zamawiającego z obsługi agregatu.

**XII. Szkolenia stacjonarne dla pracowników i kadry kierowniczej – 1 kpl.**

Przedmiotem zamówienia jest przeprowadzenie szkolenia stacjonarnego w Urzędzie Gminy Drelów dla 35 osób w dwóch grupach szkoleniowych dla pracowników JST dotyczącego bezpieczeństwa informacji, budującego świadomość cyberzagrożeń, wskazującego skutki naruszeń zasad bezpieczeństwa informacji oraz kwestie prawne związane z ochroną danych osobowych i sposobów ochrony. Celem szkolenia jest podniesienie świadomości uczestników w zakresie bezpieczeństwa informacji, umożliwiając im lepsze zrozumienie zagrożeń, skutków naruszeń i efektywne stosowanie środków bezpieczeństwa w codziennej pracy. Zamawiający zapewni salę szkoleniową wyposażoną w ekran i rzutnik, z minimalną liczbą 18 miejsc.

Wymagania:

1. Szkolenia muszą odbywać się w godzinach pracy Urzędu.

2. Wykonawca w ramach wykonania usługi przedstawi szczegółowy program szkolenia zawierający informacje dotyczące tematyki i czasu szkolenia, i dostarczy go w terminie nie później niż 7 dni roboczych przed dniem rozpoczęcia szkolenia, do akceptacji Zamawiającego.

3. Opracowane materiały będą musiały być dostarczone w formie papierowej i elektronicznej z możliwością powiększania treści. W ramach wynagrodzenia Wykonawca przygotuje i zapewni materiały szkoleniowe dla każdego uczestnika, pozwalające na samodzielną edukację z zakresu tematyki szkolenia. Zamawiający dopuszcza dostarczenie kompletu materiałów w formie elektronicznej, np. dokumenty w standardzie PDF.

4. Wykonawca dostarczy materiały szkoleniowe uczestnikom szkolenia najpóźniej w dniu rozpoczęcia szkolenia.

5. Szkolenie musi obejmować co najmniej następującą tematykę:

a. podstawy cyberbezpieczeństwa (podstawowe pojęcia i zasady działania),

b. znaczenie cyberbezpieczeństwa dla jednostki samorządu terytorialnego,

c. cyberbezpieczeństwo w codziennej pracy,

d. standardy i najlepsze praktyki postępowania w celu zapewnienia cyberbezpieczeństwa w miejscu pracy, cyberhigiena,

e. bezpieczeństwo urządzeń i bezpieczeństwo fizyczne, bezpieczne hasła, zarządzanie hasłami, uwierzytelnienie dwu- i wieloskładnikowe, klucze sprzętowe,

f. przegląd i rozpoznawanie najpopularniejszych zagrożeń w cyberprzestrzeni (w tym rodzaje ataków, ransomware i malware, phishing, oszustwa i wyłudzenia z uwzględnieniem oszustwa typu Business E-mail Compromise, atak telefoniczny, spoofing, atak odwrócony – zmuszenie ofiary do szukania pomocy u atakującego, przekręt nigeryjski, wyłudzenia BLIK, oszustwo na dyrektora/prezesa), sposoby unikania zagrożeń, zasady bezpiecznego korzystania z Internetu,

g. ochrona informacji i prywatność w Internecie,

h. jak bezpiecznie korzystać z narzędzi teleinformatycznych – przykłady stosowania zabezpieczeń,

i. reagowanie na incydenty bezpieczeństwa (w tym zasady postępowania w razie podejrzenia naruszenia bezpieczeństwa/ataku),

j. procedury zgłaszania incydentów,

k. ochrona danych osobowych i wrażliwych informacji,

l. analiza przypadków – praktyczne scenariusze,

m. omówienie zjawiska pracy zdalnej w oparciu o aktualnie obowiązujące przepisy prawa w zakresie bezpieczeństwa informacji,

n. analiza przepisów rozporządzenia Rady Ministrów z dnia 21 maja 2024 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (Dz. U. 2024 poz. 773) i ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (t.j. Dz.U. 2024 poz. 1077).

6. Forma prezentacji połączonej z warsztatami, co najmniej 40% zawartości szkolenia mają to być treści praktyczne, aktualne, angażujące i aktywizujące uczestników szkolenia, pozwalające na podniesienie umiejętności związanych z:

a. rozpoznawaniem zagrożeń i reagowanie na nie,

b. wykorzystywaniem narzędzi informatycznych zapewniających bezpieczeństwo przetwarzanych informacji oraz zabezpieczeń dla poczty elektronicznej i stron WWW,

c. radzeniem sobie w sytuacjach kryzysowych (scenariusze codziennych zagrożeń).

7. W trakcie szkolenia trener powinien odpowiadać na pytania uczestników. Dopuszczalne jest zorganizowanie sesji pytań i odpowiedzi na zakończenie szkolenia.

8. W wyniku szkolenia pracownicy mają być w stanie odróżnić typowe błędy techniczne od potencjalnego ataku, wiedzieć jak uniknąć potencjalnego zagrożenia, a w przypadku wystąpienia naruszenia – umieć podjąć podstawowe działania ograniczające skutki wystąpienia incydentu oraz zgłosić incydent do odpowiednich komórek.

9. Czas trwania szkolenia (dla jednej grupy) – min. 4 godziny lekcyjne (po 45 min.).

10. Z przeprowadzonych szkoleń Wykonawca musi przedstawić listy obecności z podpisami uczestników szkolenia.

11. Szkolenie musi być zakończone testem weryfikującym skuteczność szkolenia oraz anonimową ankietą wśród uczestników, oceniającą co najmniej przydatność szkolenia, zakres przekazanych informacji, adekwatność przekazanych informacji do potrzeb uczestników, formę prezentacji i komunikatywność prowadzącego szkolenie. Wykonawca przedstawi Zamawiającemu podsumowanie wyników ankiety.

**XIII. Szkolenia specjalistyczne dla informatyka – 1 szt.**

Przedmiotem zamówienia jest przeprowadzenie szkolenia specjalistycznego z cyberbezpieczeństwa dla informatyka.

Szkolenie musi zawierać poniższą tematykę:

1. Fundamentalne koncepcje bezpieczeństwa:

a. Koncepcje bezpieczeństwa

b. Środki kontroli bezpieczeństwa (Security Controls)

2. Porównanie typów zagrożeń:

a. Typy podmiotów zagrożenia (Threat Actors)

b. Powierzchnia ataku (Attack Surfaces)

c. Inżynieria społeczna (Social Engineering)

3. Wyjaśnianie rozwiązań kryptograficznych:

a. Algorytmy kryptograficzne

b. Publiczna infrastruktura klucza (PKI)

c. Rozwiązania kryptograficzne

4. Wdrażanie zarządzania tożsamością i kontrolą dostępu:

a. Uwierzytelnianie (Authentication)

b. Autoryzacja (Authorization)

c. Zarządzanie tożsamością (Identity Management)

5. Bezpieczna architektura sieci przedsiębiorstwa:

a. Architektura sieci przedsiębiorstwa

b. Urządzenia zabezpieczające sieć (Network Security Appliances)

c. Bezpieczna komunikacja (Secure Communications)

6. Bezpieczna architektura sieci w chmurze

a. Infrastruktura chmurowa (Cloud Infrastructure)

b. Systemy wbudowane i architektura Zero Trust (Embedded Systems and Zero Trust Architecture)

7. Wyjaśnianie koncepcji odporności i bezpieczeństwa lokalizacji:

a. Zarządzanie zasobami (Asset Management)

b. Strategie redundancji (Redundancy Strategies)

c. Bezpieczeństwo fizyczne (Physical Security)

8. Wyjaśnianie zarządzania lukami w zabezpieczeniach:

a. Luki w zabezpieczeniach urządzeń i systemów operacyjnych (Device and OS Vulnerabilities)

b. Luki w aplikacjach i środowiskach chmurowych (Application and Cloud Vulnerabilities)

c. Metody identyfikacji luk (Vulnerability Identification Methods)

d. Analiza i usuwanie luk (Vulnerability Analysis and Remediation)

9. Ocena możliwości zabezpieczeń sieci:

a. Benchmarki zabezpieczeń sieci (Network Security Baselines)

b. Wzmacnianie możliwości zabezpieczeń sieci (Network Security Capability Enhancement)

10. Ocena zabezpieczeń urządzeń końcowych:

a. Wdrażanie zabezpieczeń urządzeń końcowych (Implement Endpoint Security)

b. Utwardzanie urządzeń mobilnych (Mobile Device Hardening)

11. Wzmacnianie zabezpieczeń aplikacji:

a. Benchmarki protokołów i aplikacji (Application Protocol Security Baselines)

b. Koncepcje zabezpieczeń aplikacji chmurowych i webowych (Cloud and Web Application Security Concepts)

12. Wyjaśnianie zagadnień odpowiedzi na incydenty i monitorowania:

a. Reagowanie na incydenty (Incident Response)

b. Cyfrowe śledztwo (Digital Forensics)

c. Źródła danych (Data Sources)

d. Narzędzia monitorowania i alarmowania (Alerting and Monitoring Tools)

13. Analiza wskaźników złośliwej aktywności

a. Wskaźniki ataków złośliwego oprogramowania (Malware Attack Indicators)

b. Wskaźniki ataków fizycznych i sieciowych (Physical and Network Attack Indicators)

c. Wskaźniki ataków aplikacyjnych (Application Attack Indicators)

14. Podsumowanie zagadnień zarządzania bezpieczeństwem

a. Polityki, standardy i procedury (Policies, Standards, and Procedures)

b. Zarządzanie zmianą (Change Management)

c. Automatyzacja i orchestracja (Automation and Orchestration)

15. Wyjaśnianie procesów zarządzania ryzykiem:

a. Procesy i koncepcje zarządzania ryzykiem

b. Zarządzanie dostawcami (Vendor Management)

c. Audyty i oceny (Audits and Assessments)

16. Podsumowanie zagadnień ochrony danych i zgodności z przepisami:

a. Klasyfikacja danych i zgodność z przepisami (Data Classification and Compliance)

b. Polityki dotyczące personelu (Personnel Policies)

17. Szkolenie musi być przeprowadzone w języku polskim.

18. Szkolenie musi być zakończone certyfikowanym egzaminem oraz, przy pozytywnym wyniku z egzaminu, otrzymaniem certyfikatu Security z obszaru bezpieczeństwa zgodnym ze standardem ISO 17024 ważnym min. 3 lata.

**XIV. Opracowanie dokumentacji SZBI – 1 kpl.**

Zakres prac dotyczących dokumentacji SZBI:

1. Aktualizacja lub opracowanie (w przypadku braku dokumentu) dokumentacji Systemu Zarządzania Bezpieczeństwem Informacji (dalej zwanej „SZBI”), w skład której wchodzą następujące dokumenty:

a. Polityka Bezpieczeństwa Informacji;

b. Instrukcja zarządzania systemem informatycznym;

c. Polityka zarządzania ciągłością działania;

d. Procedura zarządzania incydentami cyberbezpieczeństwa;

e. Analiza ryzyka w zakresie Bezpieczeństwa Informacji;

2. Wdrożenie SZBI we współpracy z kierownikiem jednostki lub osobami wyznaczonymi do wdrożenia SZBI.

3. W ramach dokumentacji SZBI ujęte zostaną następujące procedury:

a. procedury kontroli dostępu

b. zabezpieczenie pomieszczeń i obiektów

c. procedury czystego biurka i ekranu

d. procedury kopii zapasowych

e. procedury ochrony logów

f. bezpieczeństwo komunikacji

g. zarządzanie bezpieczeństwem sieci

h. przesyłanie informacji

i. plany ciągłości działania

j. procedury zarządzania incydentami

k. prywatność i ochrona danych osobowych

l. szacowanie ryzyka w obszarze bezpieczeństwa informacji

m. szkolenia personelu

4. Szczegółowa zawartość dokumentacji zostanie określona w zależności od stanu faktycznego odpowiadającego strukturze i zasobom Zamawiającego i wdrażanej jednostki w oparciu o wzajemne ustalenia dokonane we współpracy pomiędzy Stronami na etapie deklaracji stosowania oraz wszelkich innych informacji uzyskanych przez Wykonawcę w trakcie realizacji Umowy mogących mieć wpływ na treść dokumentacji. Usługi dotyczące czynności wdrażających dokumentację zostanie uznana za wykonaną po przekazaniu Zleceniodawcy przez Zleceniobiorcę całości dokumentacji SZBI i podpisaniu protokołu odbioru przez Zamawiającego.

**XV. Audyt końcowy – 1 kpl.**

Wymagania dotyczące przeprowadzenie audytu końcowego:

1. Wykonawca zapewni audytora do przeprowadzenia audytu końcowego na zgodność ISO 27001, który dokona oceny funkcjonowania SZBI i przedstawi jego wyniki w raporcie z audytu.

2. Audytor musi posiadać 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;

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.

3. W ramach realizacji Przedmiotu Zamówienia Zamawiający oczekuje realizacji Audytu końcowego SZBI – termin zakończenia najpóźniej na 14 dni przed końcem realizacji umowy.

4. Audyt końcowy SZBI musi obejmować zakres:

a. Polityka i Procedury Bezpieczeństwa

i. Przeprowadzanie analizy dokumentacji dotyczącej bezpieczeństwa IT

ii. Sprawdzenie polityki bezpieczeństwa informacji

b. Przegląd dokumentacji procedur bezpieczeństwa informacji i ich skuteczności w praktyce

Zarządzanie Ryzykiem i Bezpieczeństwem

i. Ocena procesów identyfikacji, oceny i zarządzania ryzykiem

ii. Analiza skuteczności działań zapobiegawczych i kontroli ryzyka

c. Zarządzanie Zabezpieczeniem Aktywów

i. Ocena klasyfikacji aktywów informacyjnych oraz skuteczności ich ochrony

ii. Przegląd procedur związanych z identyfikacją i zabezpieczaniem aktywów

d. Bezpieczne Zarządzanie Dostępem

i. Sprawdzenie mechanizmów kontroli dostępu do systemów i danych

ii. Ocena skuteczności systemów uwierzytelniania i autoryzacji

e. Kryptografia

i. Analiza zastosowania kryptografii do ochrony poufności i integralności danych

ii. Ocena zgodności z wymaganiami dotyczącymi stosowania kryptografii

f. Bezpieczeństwo Fizyczne i Środowiskowe

i. Ocena zabezpieczeń infrastruktury fizycznej i działań zapobiegawczych przeciwko awariom i katastrofom

ii. Przegląd procedur związanych z zapewnieniem bezpieczeństwa środowiskowego

g. Bezpieczeństwo Personelu

i. Przegląd procesów selekcji, szkolenia i monitorowania personelu pod kątem bezpieczeństwa informacji

ii. Ocena świadomości pracowników na temat polityki bezpieczeństwa informacji

h. Bezpieczne Operacje

i. Ocena procedur dotyczących bezpiecznej eksploatacji systemów i usług

ii. Sprawdzenie zgodności z wymaganiami dotyczącymi bezpiecznych operacji

i. Zarządzanie Komunikacją

i. Przegląd zabezpieczeń zapewniających bezpieczny przepływ informacji wewnątrz i na zewnątrz organizacji

ii. Ocena procedur komunikacji w kontekście bezpieczeństwa informacji

j. Zarządzanie Incydentami Bezpieczeństwa Informacji

i. Sprawdzenie procedur reagowania na incydenty bezpieczeństwa informacji

ii. Analiza skuteczności działań podejmowanych w przypadku incydentów

k. Monitorowanie, Przeglądy i Audyty

i. Ocena systemu monitorowania skuteczności zarządzania bezpieczeństwem informacji

ii. Przegląd przeprowadzonych audytów i ich wyników

l. Ciągłe Doskonalenie

i. Analiza procesów ciągłego doskonalenia systemu zarządzania bezpieczeństwem informacji

ii. Ocena działań podejmowanych w celu identyfikacji i eliminacji słabych punktów

m. Opracowanie raportu zawierającego opis zidentyfikowanych niezgodności oraz obserwacji wraz z rekomendacjami

n. Opracowanie rekomendowanych zmian