ZP.271.17.2022 Załącznik Nr 9 do SWZ

OPIS PRZEDMIOTU ZAMÓWIENIA

„Dostawa sprzętu, oprogramowania, przeprowadzenie szkoleń i opracowanie diagnozy cyberbezpieczeństwa w ramach projektu „Cyfrowa Gmina”

Spis treści

Wymagania ogólne dla urządzeń i oprogramowania sieciowego.

– całość sprzętu i oprogramowania musi pochodzić z autoryzowanego kanału sprzedaży producentów;
– całość sprzętu musi być nowa, nie używana wcześniej;

Wymagania gwarancyjne.

Sprzęt

– O ile wymagania szczegółowe nie specyfikują inaczej, na dostarczany sprzęt musi być udzielona min. 24 miesięczna gwarancja (chyba, że zapisy szczegółowe stanowią inaczej) oparte na gwarancji producenta rozwiązanie; serwis gwarancyjny świadczony ma być w miejscu instalacji sprzętu; czas reakcji na zgłoszony problem (rozumiany jako podjęcie działań diagnostycznych i kontakt ze zgłaszającym) nie może przekroczyć jednego dnia roboczego;
– Wykonawca musi udostępnić pojedynczy punkt przyjmowania zgłoszeń dla dostarczanych rozwiązań. Każde zgłoszenie należy potwierdzić drogą pisemną lub elektroniczną w postaci potwierdzenia przyjęcia zgłoszenia;
– Gwarantowany czas naprawy nie może być dłuższy niż 14 dni roboczych. W przypadku sprzętu, dla którego jest wymagany dłuższy czas na naprawę sprzętu, Zamawiający wymaga podstawienia na czas naprawy Sprzętu o nie gorszych parametrach funkcjonalnych. Naprawa w takim przypadku nie może przekroczyć 30 dni roboczych od momentu zgłoszenia usterki;

Oprogramowanie

– oprogramowanie powinno posiadać min. 24-miesięczną gwarancję obejmującą swoim zakresem poprawność działania w zakresie wdrożonych funkcjonalności wg stanu na dzień podpisania stosownego protokołu odbioru (chyba że zapisy szczegółowe stanowią inaczej);

Miejsce instalacji sprzętu i oprogramowania/systemu.

– Dostarczony sprzęt i oprogramowanie powinny zostać zamontowane, zainstalowane i skonfigurowane w budynku Urzędu Gminy Markowa w miejscach wskazanych przez Zamawiającego.

Zestawienie zakresu dostaw i usług oraz minimalnych wymaganych okresów gwarancji.

Lp.	Nazwa	Minimalna długość gwarancji (m-ce)	Ilość
1.	Zapewnienie cyberbezpieczenstwa samorządowych systemów informatycznych – diagnoza cyberbezpieczeństwa.	Nie dotyczy	1
2.	Stacje robocze	36	4
3.	Zasilacz UPS	24	4
4.	Laptop	36	4
5.	System bezpieczeństwa logowania	24	1
6.	Serwer wirtualizacyjny	24	2
7.	Zasilacz awaryjny	36	1
8.	Licencja serwerowego systemu operacyjnego	24	1
9.	Licencja bezpieczeństwa danych	24	1
10.	Serwer NAS	36	1
11.	Przełącznik sieciowy	36	2
12.	Szkolenie	Nie dotyczy	1

Szczegółowy opis pozycji:

1. Zapewnienie cyberbezpieczenstwa samorządowych systemów informatycznych – diagnoza cyberbezpieczeństwa.

Dotyczy przeprowadzenia diagnozy bezpieczeństwa zgodnie z wymaganiami konkursu programu "Cyfrowa Gmina", opisanymi na stronie https://www.gov.pl/web/cppc/cyfrowa-gmina.
Wykonawca musi wykonać usługę zgodnie zakresem oraz z formularzem stanowiącym załącznik do dokumentacji konkursowej- Załącznik_nr_8__Formularz_informacji_związanych_z_przeprowadzeniem_diagnozy_cyberbezpieczeństwa.
Diagnoza musi zostać przeprowadzona przez osobę posiadającą uprawnienia wykazane w Rozporządzeniu Ministra Cyfryzacji z dnia 12 października 2018 r. w sprawie wykazu certyfikatów uprawniających do przeprowadzenia audytu.

2. Stacje robocze – szt. 4 – wymagania minimalne.

Stacja robocza o minimalnych parametrach:

- **Wydajność systemu**

Procesor wielordzeniowy zaprojektowany do pracy w komputerach stacjonarnych klasy x86, na poziomie wydajności liczonej w punktach na podstawie testów „PassMark – CPU mark" dostępnych na stronie http://www.cpubenchmark.net/. na dzień ogłoszenia postępowania. Procesor powinien osiągnąć wynik co najmniej 12000 punktów.

- **Chipset:**

Dostosowany do zaoferowanego procesora.

- Pamięć operacyjna:

Min. 8GB, typ pamięci nie starszy niż DDR4,
Min. 2 sloty na moduły pamięci umożliwiające instalację RAM do min. 16 GB.

- **Parametry pamięci masowej**

Dysk SSD o pojemności min. 500GB SSD

- **Karta graficzna**

Zintegrowana karta graficzna wykorzystująca pamięć RAM systemu dynamicznie przydzielaną na potrzeby grafiki

- **Wyposażenie multimedialne**

Interfejs wideo: min. VGA, HDMI lub DP

- **Połączenia i karty sieciowe**

Port sieci LAN 10/100/1000 Ethernet RJ 45

- **Czytnik kart**

Dołączony czytnik kart procesorowych o minimalnych parametrach:
Interfejs Hosta: min. USB 2.0, zaciski, protokół CCID
Obsługiwane standardy kart: min. ISO7816-1, 2, 3, 4; EMV terminal level 1 version 4
Obsługa kart dostarczanych w punkcie System bezpieczeństwa logowania
Do czytnika dołączony stand
Do czytnika dołączone oprogramowanie do logowania

- **System operacyjny:**

1) Zamawiający wymaga aby dostarczone oprogramowanie było fabrycznie nowe nigdy wcześniej nie instalowane i aktywowane na innym urządzeniu.
2) Wszystkie komputery mają być dostarczone z zainstalowanym lub preinstalowanym oprogramowaniem systemowym. Procedura instalacji lub preinstalacji może być dokonana zarówno przez producenta jak i sprzedawcę.
3) Zamawiający wymaga dostarczenia dokumentów potwierdzających legalność oprogramowania np. certyfikaty autentyczności wystawione przez producenta oprogramowania.
4) Zamawiający dopuszcza możliwość przeprowadzenia weryfikacji oryginalności dostarczonych programów komputerowych u Producenta oprogramowania jako elementu procedury odbioru. Weryfikacja będzie polegała na aktywowaniu oprogramowania u producenta w przypadku takich wymagań lub/i rejestracji oprogramowania na stronach producenta danego oprogramowania lub/i sprawdzeniu poprzez infolinię producenta oprogramowania numerów seryjnych itp. Procedura weryfikacji będzie zależna od możliwości udostępnianych przez producenta oprogramowania.

– **Oprogramowanie antywirusowe:**

1) Rozwiązanie musi wspierać systemy operacyjne Windows (Windows 7/Windows 8/Windows 8.1/Windows 10/Windows 11).
2) Rozwiązanie musi wspierać architekturę ARM64.
3) Rozwiązanie musi zapewniać wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor.
4) Rozwiązanie musi posiadać wbudowaną technologię do ochrony przed rootkitami oraz podłączeniem komputera do sieci botnet.
5) Rozwiązanie musi zapewniać wykrywanie potencjalnie niepożądanych, niebezpiecznych oraz podejrzanych aplikacji.
6) Rozwiązanie musi zapewniać skanowanie w czasie rzeczywistym otwieranych, zapisywanych i wykonywanych plików.
7) Rozwiązanie musi zapewniać skanowanie całego dysku, wybranych katalogów lub pojedynczych plików "na żądanie" lub według harmonogramu.
8) Rozwiązanie musi zapewniać skanowanie plików spakowanych i skompresowanych oraz dysków sieciowych i dysków przenośnych.
9) 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.
10) 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).
11) Rozwiązanie musi zapewniać skanowanie ruchu sieciowego wewnątrz szyfrowanych protokołów HTTPS, POP3S, IMAPS.
12) 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.
13) 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.

14) 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.
15) Moduł HIPS musi posiadać możliwość pracy w jednym z pięciu trybów:
    - tryb automatyczny z regułami, gdzie program automatycznie tworzy i wykorzystuje reguły wraz z możliwością wykorzystania reguł utworzonych przez użytkownika,
    - tryb interaktywny, w którym to rozwiązanie pyta użytkownika o akcję w przypadku wykrycia aktywności w systemie,
    - tryb oparty na regułach, gdzie zastosowanie mają jedynie reguły utworzone przez użytkownika,
    - 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,
    - tryb inteligentny, w którym rozwiązanie będzie powiadamiało wyłącznie o szczególnie podejrzanych zdarzeniach.
16) Rozwiązanie musi być wyposażone we wbudowaną funkcję, która wygeneruje pełny raport na temat stacji, na której zostało zainstalowane, w tym przynajmniej z: zainstalowanych aplikacji, usług systemowych, informacji o systemie operacyjnym i sprzęcie, aktywnych procesów i połączeń sieciowych, harmonogramu systemu operacyjnego, pliku hosts, sterowników.
17) 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.
18) Rozwiązanie musi posiadać automatyczną, inkrementacyjną aktualizację silnika detekcji.
19) Rozwiązanie musi posiadać tylko jeden proces uruchamiany w pamięci, z którego korzystają wszystkie funkcje systemu (antywirus, antyspyware, metody heurystyczne).
20) Rozwiązanie musi posiadać funkcjonalność skanera UEFI, który chroni użytkownika poprzez wykrywanie i blokowanie zagrożeń, atakujących jeszcze przed uruchomieniem systemu operacyjnego.

– **Administracja zdalna:**

1) Rozwiązanie musi wspierać instalację na systemach Windows Server (od 2012), Linux oraz w postaci maszyny wirtualnej w formacie OVA lub dysku wirtualnego w formacie VHD.
2) Rozwiązanie musi zapewniać instalację z użyciem nowego lub istniejącego serwera bazy danych MS SQL i MySQL.
3) Rozwiązanie musi zapewniać pobranie wszystkich wymaganych elementów serwera centralnej administracji w postaci jednego pakietu instalacyjnego i każdego z modułów oddzielnie bezpośrednio ze strony producenta.
4) Rozwiązanie musi zapewniać dostęp do konsoli centralnego zarządzania w języku polskim z poziomu interfejsu WWW zabezpieczony za pośrednictwem protokołu SSL.
5) Rozwiązanie musi zapewniać zabezpieczoną komunikację pomiędzy poszczególnymi modułami serwera za pomocą certyfikatów.

6) Rozwiązanie musi zapewniać utworzenia własnego CA (Certification Authority) oraz dowolnej liczby certyfikatów z podziałem na typ elementu: agent, serwer zarządzający, serwer proxy, moduł zarządzania urządzeniami mobilnymi.
7) Rozwiązanie musi wspierać zarządzanie urządzeniami z systemem iOS i Android.
8) Rozwiązanie musi zapewniać centralną konfigurację i zarządzanie przynajmniej takimi modułami jak: ochrona antywirusowa, antyspyware, które działają na stacjach roboczych w sieci.
9) Rozwiązanie musi zapewniać weryfikację podzespołów zarządzanego komputera (w tym przynajmniej: producent, model, numer seryjny, informacje o systemie, procesor, pamięć RAM, wykorzystanie dysku twardego, informacje o wyświetlaczu, urządzenia peryferyjne, urządzenia audio, drukarki, karty sieciowe, urządzenia masowe).
10) Rozwiązanie musi zapewniać instalowanie i odinstalowywanie oprogramowania firm trzecich dla systemów Windows oraz MacOS oraz odinstalowywanie oprogramowania zabezpieczającego firm trzecich, zgodnych z technologią OPSWAT.
11) Rozwiązanie musi zapewniać wymuszenia dwufazowej autoryzacji podczas logowania do konsoli administracyjnej.
12) Serwer administracyjny musi posiadać możliwość tworzenia grup statycznych i dynamicznych komputerów.
13) 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.
14) Rozwiązanie musi zapewniać korzystanie z minimum 100 szablonów raportów, przygotowanych przez producenta oraz musi zapewniać tworzenie własnych raportów przez administratora.
15) Rozwiązanie musi zapewniać wysłanie powiadomienia przynajmniej za pośrednictwem wiadomości email, komunikatu SNMP oraz do dziennika syslog.
16) Rozwiązanie musi zapewniać podział uprawnień administratorów w taki sposób, aby każdy z nich miał możliwość zarządzania konkretnymi grupami komputerów, politykami oraz zadaniami.

– **Ochrona serwera**

1) Rozwiązanie musi wspierać systemy Microsoft Windows Server 2012 i nowszych oraz Linux w tym co najmniej: RedHat Enterprise Linux (RHEL) 7 i 8, CentOS 7 i 8, Ubuntu Server 16.04 LTS i nowsze, Debian 9, Debian 10, SUSE Linux Enterprise Server (SLES) 12, SUSE Linux Enterprise Server (SLES) 15, Oracle Linux oraz Amazon Linux.
2) Rozwiązanie musi zapewniać ochronę przed wirusami, trojanami, robakami i innymi zagrożeniami.
3) Rozwiązanie musi zapewniać wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor.
4) Rozwiązanie musi zapewniać możliwość skanowania dysków sieciowych typu NAS.
5) 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.

6) Rozwiązanie musi wspierać automatyczną, inkrementacyjną aktualizację silnika detekcji.
7) Rozwiązanie musi posiadać możliwość wykluczania ze skanowania procesów.
8) Rozwiązanie musi posiadać możliwość określenia typu podejrzanych plików, jakie będą przesyłane do producenta, w tym co najmniej pliki wykonywalne, archiwa, skrypty, dokumenty.
9) Dodatkowe wymagania dla ochrony serwerów Windows:
10) Rozwiązanie musi posiadać możliwość skanowania plików i folderów, znajdujących się w usłudze chmurowej OneDrive.
11) Rozwiązanie musi posiadać system zapobiegania włamaniom działający na hoście (HIPS).
12) Rozwiązanie musi wspierać skanowanie magazynu Hyper-V.
13) Rozwiązanie musi posiadać funkcjonalność skanera UEFI, który chroni użytkownika poprzez wykrywanie i blokowanie zagrożeń, atakujących jeszcze przed uruchomieniem systemu operacyjnego.
14) 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.
15) Rozwiązanie musi automatyczne wykrywać usługi zainstalowane na serwerze i tworzyć dla nich odpowiednie wyjątki.
16) Rozwiązanie musi posiadać wbudowany system IDS z detekcją prób ataków, anomalii w pracy sieci oraz wykrywaniem aktywności wirusów sieciowych.
17) Rozwiązanie musi zapewniać możliwość dodawania wyjątków dla systemu IDS, co najmniej w oparciu o występujący alert, kierunek, aplikacje, czynność oraz adres IP.
18) Rozwiązanie musi posiadać ochronę przed oprogramowaniem wymuszającym okup za pomocą dedykowanego modułu.

– **Oprogramowanie biurowe:**

Licencja na pakiet aplikacji biurowych nie może być ograniczona czasowo. Praca na aplikacjach zawartych w pakiecie musi być możliwa także bez połączenia z siecią Internet.

<u>Pakiet biurowy musi spełniać następujące wymagania:</u>

1) Wymagania odnośnie interfejsu użytkownika:
   a) Pełna polska wersja językowa interfejsu użytkownika
   b) Prostota i intuicyjność obsługi, pozwalająca na pracę osobom nieposiadającym umiejętności technicznych
   c) Możliwość zintegrowania uwierzytelniania użytkowników z usługą katalogową (Active Directory lub funkcjonalnie równoważną) – użytkownik raz zalogowany z poziomu systemu operacyjnego stacji roboczej ma być automatycznie rozpoznawany we wszystkich modułach oferowanego rozwiązania bez potrzeby oddzielnego monitowania go o ponowne uwierzytelnienie się.
2) Oprogramowanie musi umożliwiać tworzenie i edycję dokumentów elektronicznych w ustalonym formacie, który spełnia następujące warunki:
   a) posiada kompletny i publicznie dostępny opis formatu,
   b) ma zdefiniowany układ informacji w postaci XML zgodnie z Tabelą B1 załącznika 2 Rozporządzenia w sprawie minimalnych wymagań dla systemów teleinformatycznych (Dz.U.05.212.1766)
   c) umożliwia wykorzystanie schematów XML

d) wspiera w swojej specyfikacji podpis elektroniczny zgodnie z Tabelą A.1.1 załącznika 2 Rozporządzenia w sprawie minimalnych wymagań dla systemów teleinformatycznych (Dz.U.05.212.1766)

3) Oprogramowanie musi umożliwiać dostosowanie dokumentów i szablonów do potrzeb instytucji oraz udostępniać narzędzia umożliwiające dystrybucję odpowiednich szablonów do właściwych odbiorców.
4) W skład oprogramowania muszą wchodzić narzędzia programistyczne umożliwiające automatyzację pracy i wymianę danych pomiędzy dokumentami i aplikacjami (język makropoleceń, język skryptowy)
5) Do aplikacji musi być dostępna pełna dokumentacja w języku polskim.
6) Pakiet zintegrowanych aplikacji biurowych musi zawierać:
   a) Edytor tekstów
   b) Arkusz kalkulacyjny
   c) Narzędzie do przygotowywania i prowadzenia prezentacji
   d) Narzędzie do zarządzania informacją prywatą (pocztą elektroniczną, kalendarzem, kontaktami i zadaniami)
7) Edytor tekstów musi umożliwiać:
   a) Edycję i formatowanie tekstu w języku polskim wraz z obsługą języka polskiego w zakresie sprawdzania pisowni i poprawności gramatycznej oraz funkcjonalnością słownika wyrazów bliskoznacznych i autokorekty
   b) Wstawianie oraz formatowanie tabel
   c) Wstawianie oraz formatowanie obiektów graficznych
   d) Wstawianie wykresów i tabel z arkusza kalkulacyjnego (wliczając tabele przestawne)
   e) Automatyczne numerowanie rozdziałów, punktów, akapitów, tabel i rysunków
   f) Automatyczne tworzenie spisów treści
   g) Formatowanie nagłówków i stopek stron
   h) Sprawdzanie pisowni w języku polskim
   i) Śledzenie zmian wprowadzonych przez użytkowników
   j) Nagrywanie, tworzenie i edycję makr automatyzujących wykonywanie czynności
   k) Określenie układu strony (pionowa/pozioma)
   l) Wydruk dokumentów
   m) Wykonywanie korespondencji seryjnej bazując na danych adresowych pochodzących z arkusza kalkulacyjnego i z narzędzia do zarządzania informacją prywatną
   n) Pracę na dokumentach utworzonych przy pomocy Microsoft Word 2003 lub Microsoft Word 2007 i 2010 z zapewnieniem bezproblemowej konwersji wszystkich elementów i atrybutów dokumentu
   o) Zabezpieczenie dokumentów hasłem przed odczytem oraz przed wprowadzaniem modyfikacji
   p) Wymagana jest dostępność do oferowanego edytora tekstu bezpłatnych narzędzi umożliwiających wykorzystanie go, jako środowiska udostępniającego formularze bazujące na schematach XML z Centralnego Repozytorium Wzorów Dokumentów Elektronicznych, które po wypełnieniu umożliwiają zapisanie pliku XML w zgodzie z obowiązującym prawem.
   q) Wymagana jest dostępność do oferowanego edytora tekstu bezpłatnych narzędzi (kontrolki) umożliwiających podpisanie podpisem elektronicznym pliku z zapisanym

dokumentem przy pomocy certyfikatu kwalifikowanego zgodnie z wymaganiami obowiązującego w Polsce prawa.

r) Wymagana jest dostępność do oferowanego edytora tekstu bezpłatnych narzędzi umożliwiających wykorzystanie go, jako środowiska udostępniającego formularze i pozwalające zapisać plik wynikowy w zgodzie z Rozporządzeniem o Aktach Normatywnych i Prawnych.

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

9) Narzędzie do przygotowywania i prowadzenia prezentacji musi umożliwiać:
   a) Przygotowywanie prezentacji multimedialnych,
   b) Prezentowanie przy użyciu projektora multimedialnego
   c) Drukowanie w formacie umożliwiającym robienie notatek
   d) Zapisanie jako prezentacja tylko do odczytu.
   e) Nagrywanie narracji i dołączanie jej do prezentacji
   f) Opatrywanie slajdów notatkami dla prezentera
   g) Umieszczanie i formatowanie tekstów, obiektów graficznych, tabel, nagrań dźwiękowych i wideo
   h) Umieszczanie tabel i wykresów pochodzących z arkusza kalkulacyjnego
   i) Odświeżenie wykresu znajdującego się w prezentacji po zmianie danych w źródłowym arkuszu kalkulacyjnym
   j) Możliwość tworzenia animacji obiektów i całych slajdów
   k) Prowadzenie prezentacji w trybie prezentera, gdzie slajdy są widoczne na jednym monitorze lub projektorze, a na drugim widoczne są slajdy i notatki prezentera

l) Pełna zgodność z formatami plików utworzonych za pomocą oprogramowania MS PowerPoint 2003, MS PowerPoint 2007 i 2010.

10) Narzędzie do zarządzania informacją prywatną (pocztą elektroniczną, kalendarzem, kontaktami i zadaniami) musi umożliwiać:

a) Pobieranie i wysyłanie poczty elektronicznej z serwera pocztowego
b) Filtrowanie niechcianej poczty elektronicznej (SPAM) oraz określanie listy zablokowanych i bezpiecznych nadawców
c) Tworzenie katalogów, pozwalających katalogować pocztę elektroniczną
d) Automatyczne grupowanie poczty o tym samym tytule
e) Tworzenie reguł przenoszących automatycznie nową pocztę elektroniczną do określonych katalogów bazując na słowach zawartych w tytule, adresie nadawcy i odbiorcy
f) Oflagowanie poczty elektronicznej z określeniem terminu przypomnienia
g) Zarządzanie kalendarzem
h) Udostępnianie kalendarza innym użytkownikom
i) Przeglądanie kalendarza innych użytkowników
j) Zapraszanie uczestników na spotkanie, co po ich akceptacji powoduje automatyczne wprowadzenie spotkania w ich kalendarzach
k) Zarządzanie listą zadań
l) Zlecanie zadań innym użytkownikom
m) Zarządzanie listą kontaktów
n) Udostępnianie listy kontaktów innym użytkownikom
o) Przeglądanie listy kontaktów innych użytkowników
p) Możliwość przesyłania kontaktów innym użytkowników

– **Certyfikaty i standardy**

- Certyfikat ISO9001:2000 dla producenta sprzętu
- Deklaracja zgodności CE
- Certyfikat TCO

✓ Klawiatura USB w układzie polskim programisty wyposażona w przewód połączeniowy o długości min. 1,2m
✓ Mysz optyczna USB z klawiszami oraz rolką (scroll) wyposażona w przewód połączeniowy o długości min. 1,2m
✓ Firma serwisująca stację roboczą musi posiadać ISO 9001:2000 – dokumenty potwierdzające należy załączyć na żądanie Zamawiającego wraz z dostawą urządzeń.
✓ Zapewnienie strony producenta na której po wpisaniu numeru seryjnego dostarczonego komputera można będzie sprawdzić fabryczną konfigurację, termin obowiązywania gwarancji oraz pobrać sterowniki do zainstalowanego systemu operacyjnego.
✓ Monitor o parametrach nie gorszych niż:
✓ Rozmiar matrycy w zakresie . 23,5” – 27”
✓ Rozdzielczość nominalna: min. 1920 x 1080 (Full HD)
✓ Format obrazu: 16:9
✓ Kontrast: min. 3000:1 (statyczny)
✓ Jasność: min. 250 cd/m²
✓ Ilość wyświetlanych kolorów: min. 16.7 mln
✓ Możliwość montażu na ścianie – standard VESA 100x100
✓ Czas reakcji matrycy GTG: maks. 4 ms

- ✓ Kąty widoczności (pion/poziom): min. 175 st. / min. 175 st.
- ✓ Regulacja pochylenia monitora: w zakresie min. 25 st.
- ✓ Rodzaj i ilość złącz video: analogowe VGA - min. 1 szt., cyfrowe HDMI lub typu DVI - min. 1 szt.
- ✓ Zastosowane technologie ochrony oczu: redukcja migotania, filtr światła niebieskiego
- ✓ Dołączony przewód zasilający oraz przewód sygnałowy do oferowanego komputera o długości min. 1m

Gwarancja: minimum 36 miesięcy.

3. Zasilacz UPS – szt. 4 – wymagania minimalne

Moc pozorna min. 850 VA
Moc rzeczywista min. 480 W
Topologia Line-interactive
Liczba, typ gniazd wyjściowych min. 4 x IEC320 C13 (10A)
Typ gniazda wejściowego min. 1 x IEC320 C14 (10A)
Czas podtrzymania przy 100 W obciążenia min. 27 min
Kształt napięcia fala impulsowa
Zimny start
Ochrona przed głębokim rozładowaniem
Ochrona Lini danych min. Internet/Tel./Faks.
Interfejs komunikacyjny min. USB
Sygnały akustyczne: min. tryb bateryjny, niski stan naładowania baterii, przeciążenie, wymiana baterii, awaria

Gwarancja min. 24 miesiące

4. Laptop

4.1. Laptop – szt. 1 – minimalne wymagania

1) Procesor wielordzeniowy ze zintegrowaną grafiką, zaprojektowany do pracy w komputerach przenośnych klasy x86, na poziomie wydajności liczonej w punktach na podstawie testów „PassMark – CPU mark" dostępnych na stronie http://www.cpubenchmark.net/.
   Procesor powinien osiągnąć wynik co najmniej 13400 punktów.
2) wielkość pamięci RAM min. 16 GB DDR4 min. 2400MHz
3) dysk twardy: min. SSD 512 GB typu SATA lub M.2
4) szyfrowanie min. TPM 2.0
5) przekątna ekranu: w zakresie 14-15,6 cali, matryca matowa, rozdzielczość min. 1920 x 1080 (Full HD) pikseli
6) wyjścia karty graficznej min. 1 x wyjście HDMI
7) wbudowane interfejsy: min. 3 x USB w tym min. 1x USB C
8) wbudowany Bluetooth
9) wbudowana karta dźwiękowa
10) wbudowany mikrofon, kamera
11) wbudowany LAN min. 1 Gbps

12) wbudowane Wi-Fi
13) wbudowany czytnik kart microSD lub SD
14) zasilanie: sieć, bateria
15) dołączony czytnik kart procesorowych o minimalnych parametrach:
    - Interfejs Hosta: min. USB 2.0, zaciski, protokół CCID
    - Obsługiwane standardy kart: min. ISO7816-1, 2, 3, 4; EMV terminal level 1 version 4
    - Obsługa kart dostarczanych w punkcie System bezpieczeństwa logowania
    - Do czytnika dołączony stand
    - Do czytnika dołączone oprogramowanie do logowania

– **System operacyjny:**

1) Zamawiający wymaga aby dostarczone oprogramowanie było fabrycznie nowe nigdy wcześniej nie instalowane i aktywowane na innym urządzeniu.
2) Wszystkie komputery mają być dostarczone z zainstalowanym lub preinstalowanym oprogramowaniem systemowym. Procedura instalacji lub preinstalacji może być dokonana zarówno przez producenta jak i sprzedawcę.
3) Zamawiający wymaga dostarczenia dokumentów potwierdzających legalność oprogramowania np. certyfikaty autentyczności wystawione przez producenta oprogramowania.
4) Zamawiający dopuszcza możliwość przeprowadzenia weryfikacji oryginalności dostarczonych programów komputerowych u Producenta oprogramowania jako elementu procedury odbioru. Weryfikacja będzie polegała na aktywowaniu oprogramowania u producenta w przypadku takich wymagań lub/i rejestracji oprogramowania na stronach producenta danego oprogramowania lub/i sprawdzeniu poprzez infolinię producenta oprogramowania numerów seryjnych itp. Procedura weryfikacji będzie zależna od możliwości udostępnianych przez producenta oprogramowania.

– **Oprogramowanie antywirusowe:**

1) Rozwiązanie musi wspierać systemy operacyjne Windows (Windows 7/Windows 8/Windows 8.1/Windows 10/Windows 11).
2) Rozwiązanie musi wspierać architekturę ARM64.
3) Rozwiązanie musi zapewniać wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor.
4) Rozwiązanie musi posiadać wbudowaną technologię do ochrony przed rootkitami oraz podłączeniem komputera do sieci botnet.
5) Rozwiązanie musi zapewniać wykrywanie potencjalnie niepożądanych, niebezpiecznych oraz podejrzanych aplikacji.
6) Rozwiązanie musi zapewniać skanowanie w czasie rzeczywistym otwieranych, zapisywanych i wykonywanych plików.
7) Rozwiązanie musi zapewniać skanowanie całego dysku, wybranych katalogów lub pojedynczych plików "na żądanie" lub według harmonogramu.
8) Rozwiązanie musi zapewniać skanowanie plików spakowanych i skompresowanych oraz dysków sieciowych i dysków przenośnych.
9) 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.

10) 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).
11) Rozwiązanie musi zapewniać skanowanie ruchu sieciowego wewnątrz szyfrowanych protokołów HTTPS, POP3S, IMAPS.
12) 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.
13) 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.
14) 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.
15) Moduł HIPS musi posiadać możliwość pracy w jednym z pięciu trybów:
    - tryb automatyczny z regułami, gdzie program automatycznie tworzy i wykorzystuje reguły wraz z możliwością wykorzystania reguł utworzonych przez użytkownika,
    - tryb interaktywny, w którym to rozwiązanie pyta użytkownika o akcję w przypadku wykrycia aktywności w systemie,
    - tryb oparty na regułach, gdzie zastosowanie mają jedynie reguły utworzone przez użytkownika,
    - 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,
    - tryb inteligentny, w którym rozwiązanie będzie powiadamiało wyłącznie o szczególnie podejrzanych zdarzeniach.
16) Rozwiązanie musi być wyposażone we wbudowaną funkcję, która wygeneruje pełny raport na temat stacji, na której zostało zainstalowane, w tym przynajmniej z: zainstalowanych aplikacji, usług systemowych, informacji o systemie operacyjnym i sprzęcie, aktywnych procesów i połączeń sieciowych, harmonogramu systemu operacyjnego, pliku hosts, sterowników.
17) 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.
18) Rozwiązanie musi posiadać automatyczną, inkrementacyjną aktualizację silnika detekcji.
19) Rozwiązanie musi posiadać tylko jeden proces uruchamiany w pamięci, z którego korzystają wszystkie funkcje systemu (antywirus, antyspyware, metody heurystyczne).
20) Rozwiązanie musi posiadać funkcjonalność skanera UEFI, który chroni użytkownika poprzez wykrywanie i blokowanie zagrożeń, atakujących jeszcze przed uruchomieniem systemu operacyjnego.

– **Administracja zdalna:**

1) Rozwiązanie musi wspierać instalację na systemach Windows Server (od 2012), Linux oraz w postaci maszyny wirtualnej w formacie OVA lub dysku wirtualnego w formacie VHD.

2) Rozwiązanie musi zapewniać instalację z użyciem nowego lub istniejącego serwera bazy danych MS SQL i MySQL.
3) Rozwiązanie musi zapewniać pobranie wszystkich wymaganych elementów serwera centralnej administracji w postaci jednego pakietu instalacyjnego i każdego z modułów oddzielnie bezpośrednio ze strony producenta.
4) Rozwiązanie musi zapewniać dostęp do konsoli centralnego zarządzania w języku polskim z poziomu interfejsu WWW zabezpieczony za pośrednictwem protokołu SSL.
5) Rozwiązanie musi zapewniać zabezpieczoną komunikację pomiędzy poszczególnymi modułami serwera za pomocą certyfikatów.
6) Rozwiązanie musi zapewniać utworzenia własnego CA (Certification Authority) oraz dowolnej liczby certyfikatów z podziałem na typ elementu: agent, serwer zarządzający, serwer proxy, moduł zarządzania urządzeniami mobilnymi.
7) Rozwiązanie musi wspierać zarządzanie urządzeniami z systemem iOS i Android.
8) Rozwiązanie musi zapewniać centralną konfigurację i zarządzanie przynajmniej takimi modułami jak: ochrona antywirusowa, antyspyware, które działają na stacjach roboczych w sieci.
9) Rozwiązanie musi zapewniać weryfikację podzespołów zarządzanego komputera (w tym przynajmniej: producent, model, numer seryjny, informacje o systemie, procesor, pamięć RAM, wykorzystanie dysku twardego, informacje o wyświetlaczu, urządzenia peryferyjne, urządzenia audio, drukarki, karty sieciowe, urządzenia masowe).
10) Rozwiązanie musi zapewniać instalowanie i odinstalowywanie oprogramowania firm trzecich dla systemów Windows oraz MacOS oraz odinstalowywanie oprogramowania zabezpieczającego firm trzecich, zgodnych z technologią OPSWAT.
11) Rozwiązanie musi zapewniać wymuszenia dwufazowej autoryzacji podczas logowania do konsoli administracyjnej.
12) Serwer administracyjny musi posiadać możliwość tworzenia grup statycznych i dynamicznych komputerów.
13) 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.
14) Rozwiązanie musi zapewniać korzystanie z minimum 100 szablonów raportów, przygotowanych przez producenta oraz musi zapewniać tworzenie własnych raportów przez administratora.
15) Rozwiązanie musi zapewniać wysłanie powiadomienia przynajmniej za pośrednictwem wiadomości email, komunikatu SNMP oraz do dziennika syslog.
16) Rozwiązanie musi zapewniać podział uprawnień administratorów w taki sposób, aby każdy z nich miał możliwość zarządzania konkretnymi grupami komputerów, politykami oraz zadaniami.

– **Ochrona serwera**

1) Rozwiązanie musi wspierać systemy Microsoft Windows Server 2012 i nowszych oraz Linux w tym co najmniej: RedHat Enterprise Linux (RHEL) 7 i 8, CentOS 7 i 8, Ubuntu Server 16.04 LTS i nowsze, Debian 9, Debian 10, SUSE Linux Enterprise Server (SLES) 12, SUSE Linux Enterprise Server (SLES) 15, Oracle Linux oraz Amazon Linux.

2) Rozwiązanie musi zapewniać ochronę przed wirusami, trojanami, robakami i innymi zagrożeniami.
3) Rozwiązanie musi zapewniać wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor.
4) Rozwiązanie musi zapewniać możliwość skanowania dysków sieciowych typu NAS.
5) 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.
6) Rozwiązanie musi wspierać automatyczną, inkrementacyjną aktualizację silnika detekcji.
7) Rozwiązanie musi posiadać możliwość wykluczania ze skanowania procesów.
8) Rozwiązanie musi posiadać możliwość określenia typu podejrzanych plików, jakie będą przesyłane do producenta, w tym co najmniej pliki wykonywalne, archiwa, skrypty, dokumenty.

Dodatkowe wymagania dla ochrony serwerów Windows:

9) Rozwiązanie musi posiadać możliwość skanowania plików i folderów, znajdujących się w usłudze chmurowej OneDrive.
10) Rozwiązanie musi posiadać system zapobiegania włamaniom działający na hoście (HIPS).
11) Rozwiązanie musi wspierać skanowanie magazynu Hyper-V.
12) Rozwiązanie musi posiadać funkcjonalność skanera UEFI, który chroni użytkownika poprzez wykrywanie i blokowanie zagrożeń, atakujących jeszcze przed uruchomieniem systemu operacyjnego.
13) 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.
14) Rozwiązanie musi automatyczne wykrywać usługi zainstalowane na serwerze i tworzyć dla nich odpowiednie wyjątki.
15) Rozwiązanie musi posiadać wbudowany system IDS z detekcją prób ataków, anomalii w pracy sieci oraz wykrywaniem aktywności wirusów sieciowych.
16) Rozwiązanie musi zapewniać możliwość dodawania wyjątków dla systemu IDS, co najmniej w oparciu o występujący alert, kierunek, aplikacje, czynność oraz adres IP.
17) Rozwiązanie musi posiadać ochronę przed oprogramowaniem wymuszającym okup za pomocą dedykowanego modułu.

– **Oprogramowanie biurowe:**

Licencja na pakiet aplikacji biurowych nie może być ograniczona czasowo. Praca na aplikacjach zawartych w pakiecie musi być możliwa także bez połączenia z siecią Internet.

Pakiet biurowy musi spełniać następujące wymagania:

1) Wymagania odnośnie interfejsu użytkownika:
   a) Pełna polska wersja językowa interfejsu użytkownika
   b) Prostota i intuicyjność obsługi, pozwalająca na pracę osobom nieposiadającym umiejętności technicznych
   c) Możliwość zintegrowania uwierzytelniania użytkowników z usługą katalogową (Active Directory lub funkcjonalnie równoważną) – użytkownik raz zalogowany z poziomu systemu

operacyjnego stacji roboczej ma być automatycznie rozpoznawany we wszystkich modułach oferowanego rozwiązania bez potrzeby oddzielnego monitowania go o ponowne uwierzytelnienie się.

2) Oprogramowanie musi umożliwiać tworzenie i edycję dokumentów elektronicznych w ustalonym formacie, który spełnia następujące warunki:
   a) posiada kompletny i publicznie dostępny opis formatu,
   b) ma zdefiniowany układ informacji w postaci XML zgodnie z Tabelą B1 załącznika 2 Rozporządzenia w sprawie minimalnych wymagań dla systemów teleinformatycznych (Dz.U.05.212.1766)
   c) umożliwia wykorzystanie schematów XML
   d) wspiera w swojej specyfikacji podpis elektroniczny zgodnie z Tabelą A.1.1 załącznika 2 Rozporządzenia w sprawie minimalnych wymagań dla systemów teleinformatycznych (Dz.U.05.212.1766)
3) Oprogramowanie musi umożliwiać dostosowanie dokumentów i szablonów do potrzeb instytucji oraz udostępniać narzędzia umożliwiające dystrybucję odpowiednich szablonów do właściwych odbiorców.
4) W skład oprogramowania muszą wchodzić narzędzia programistyczne umożliwiające automatyzację pracy i wymianę danych pomiędzy dokumentami i aplikacjami (język makropoleceń, język skryptowy)
5) Do aplikacji musi być dostępna pełna dokumentacja w języku polskim.
6) Pakiet zintegrowanych aplikacji biurowych musi zawierać:
   a) Edytor tekstów
   b) Arkusz kalkulacyjny
   c) Narzędzie do przygotowywania i prowadzenia prezentacji
   d) Narzędzie do zarządzania informacją prywatą (pocztą elektroniczną, kalendarzem, kontaktami i zadaniami)
7) Edytor tekstów musi umożliwiać:
   a) Edycję i formatowanie tekstu w języku polskim wraz z obsługą języka polskiego w zakresie sprawdzania pisowni i poprawności gramatycznej oraz funkcjonalnością słownika wyrazów bliskoznacznych i autokorekty
   b) Wstawianie oraz formatowanie tabel
   c) Wstawianie oraz formatowanie obiektów graficznych
   d) Wstawianie wykresów i tabel z arkusza kalkulacyjnego (wliczając tabele przestawne)
   e) Automatyczne numerowanie rozdziałów, punktów, akapitów, tabel i rysunków
   f) Automatyczne tworzenie spisów treści
   g) Formatowanie nagłówków i stopek stron
   h) Sprawdzanie pisowni w języku polskim
   i) Śledzenie zmian wprowadzonych przez użytkowników
   j) Nagrywanie, tworzenie i edycję makr automatyzujących wykonywanie czynności
   k) Określenie układu strony (pionowa/pozioma)
   l) Wydruk dokumentów
   m) Wykonywanie korespondencji seryjnej bazując na danych adresowych pochodzących z arkusza kalkulacyjnego i z narzędzia do zarządzania informacją prywatną

n) Pracę na dokumentach utworzonych przy pomocy Microsoft Word 2003 lub Microsoft Word 2007 i 2010 z zapewnieniem bezproblemowej konwersji wszystkich elementów i atrybutów dokumentu
o) Zabezpieczenie dokumentów hasłem przed odczytem oraz przed wprowadzaniem modyfikacji
p) Wymagana jest dostępność do oferowanego edytora tekstu bezpłatnych narzędzi umożliwiających wykorzystanie go, jako środowiska udostępniającego formularze bazujące na schematach XML z Centralnego Repozytorium Wzorów Dokumentów Elektronicznych, które po wypełnieniu umożliwiają zapisanie pliku XML w zgodzie z obowiązującym prawem.
q) Wymagana jest dostępność do oferowanego edytora tekstu bezpłatnych narzędzi (kontrolki) umożliwiających podpisanie podpisem elektronicznym pliku z zapisanym dokumentem przy pomocy certyfikatu kwalifikowanego zgodnie z wymaganiami obowiązującego w Polsce prawa.
r) Wymagana jest dostępność do oferowanego edytora tekstu bezpłatnych narzędzi umożliwiających wykorzystanie go, jako środowiska udostępniającego formularze i pozwalające zapisać plik wynikowy w zgodzie z Rozporządzeniem o Aktach Normatywnych i Prawnych.

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

9) Narzędzie do przygotowywania i prowadzenia prezentacji musi umożliwiać:
a) Przygotowywanie prezentacji multimedialnych,
b) Prezentowanie przy użyciu projektora multimedialnego

c) Drukowanie w formacie umożliwiającym robienie notatek
d) Zapisanie jako prezentacja tylko do odczytu
e) Nagrywanie narracji i dołączanie jej do prezentacji
f) Opatrywanie slajdów notatkami dla prezentera
g) Umieszczanie i formatowanie tekstów, obiektów graficznych, tabel, nagrań dźwiękowych i wideo
h) Umieszczanie tabel i wykresów pochodzących z arkusza kalkulacyjnego
i) Odświeżenie wykresu znajdującego się w prezentacji po zmianie danych w źródłowym arkuszu kalkulacyjnym
j) Możliwość tworzenia animacji obiektów i całych slajdów
k) Prowadzenie prezentacji w trybie prezentera, gdzie slajdy są widoczne na jednym monitorze lub projektorze, a na drugim widoczne są slajdy i notatki prezentera
l) Pełna zgodność z formatami plików utworzonych za pomocą oprogramowania MS PowerPoint 2003, MS PowerPoint 2007 i 2010.

10) Narzędzie do zarządzania informacją prywatną (pocztą elektroniczną, kalendarzem, kontaktami i zadaniami) musi umożliwiać:
a) Pobieranie i wysyłanie poczty elektronicznej z serwera pocztowego
b) Filtrowanie niechcianej poczty elektronicznej (SPAM) oraz określanie listy zablokowanych i bezpiecznych nadawców
c) Tworzenie katalogów, pozwalających katalogować pocztę elektroniczną
d) Automatyczne grupowanie poczty o tym samym tytule
e) Tworzenie reguł przenoszących automatycznie nową pocztę elektroniczną do określonych katalogów bazując na słowach zawartych w tytule, adresie nadawcy i odbiorcy
f) Oflagowanie poczty elektronicznej z określeniem terminu przypomnienia
g) Zarządzanie kalendarzem
h) Udostępnianie kalendarza innym użytkownikom
i) Przeglądanie kalendarza innych użytkowników
j) Zapraszanie uczestników na spotkanie, co po ich akceptacji powoduje automatyczne wprowadzenie spotkania w ich kalendarzach
k) Zarządzanie listą zadań
l) Zlecanie zadań innym użytkownikom
m) Zarządzanie listą kontaktów
n) Udostępnianie listy kontaktów innym użytkownikom
o) Przeglądanie listy kontaktów innych użytkowników
p) Możliwość przesyłania kontaktów innym użytkowników

4.2. Laptop - szt. 3 – minimalne wymagania:

1) Procesor wielordzeniowy ze zintegrowaną grafiką, zaprojektowany do pracy w komputerach przenośnych klasy x86, na poziomie wydajności liczonej w punktach na podstawie testów „PassMark – CPU mark" dostępnych na stronie http://www.cpubenchmark.net/.
Procesor powinien osiągnąć wynik co najmniej 7500 punktów.
2) wielkość pamięci RAM 8 GB DDR4 min. 2400MHz, pamięć RAM rozszerzalna do min. 16 GB
3) dysk twardy: SSD 256 GB typu SATA lub M.2
4) przekątna ekranu: w zakresie 14-15,6 cali

5) rozdzielczość min. 1920 x 1080 (Full HD) pikseli
6) wyjścia karty graficznej min. 1 x wyjście HDMI
7) wbudowane interfejsy: min. 3 x USB
8) wbudowany Bluetooth
9) wbudowana karta dźwiękowa
10) wbudowany mikrofon
11) wbudowany LAN min. 1 Gbps
12) wbudowane Wi-Fi
13) wbudowany czytnik kart microSD lub SD
14) zasilanie: sieć, bateria
15) dołączony czytnik kart procesorowych o minimalnych prametrach:
    - Interfejs Hosta: min. USB 2.0, zaciski, protokół CCID
    - Obsługiwane standardy kart: min. ISO7816-1, 2, 3, 4; EMV terminal level 1 version 4
    - Obsługa kart dostarczanych w punkcie System bezpieczeństwa logowania
    - Do czytnika dołączony stand
    - Do czytnika dołączone oprogramowanie do logowania

– **System operacyjny:**

1) Zamawiający wymaga aby dostarczone oprogramowanie było fabrycznie nowe nigdy wcześniej nie instalowane i aktywowane na innym urządzeniu.
2) Wszystkie komputery mają być dostarczone z zainstalowanym lub preinstalowanym oprogramowaniem systemowym. Procedura instalacji lub preinstalacji może być dokonana zarówno przez producenta jak i sprzedawcę.
3) Zamawiający wymaga dostarczenia dokumentów potwierdzających legalność oprogramowania np. certyfikaty autentyczności wystawione przez producenta oprogramowania.
4) Zamawiający dopuszcza możliwość przeprowadzenia weryfikacji oryginalności dostarczonych programów komputerowych u Producenta oprogramowania jako elementu procedury odbioru. Weryfikacja będzie polegała na aktywowaniu oprogramowania u producenta w przypadku takich wymagań lub/i rejestracji oprogramowania na stronach producenta danego oprogramowania lub/i sprawdzeniu poprzez infolinię producenta oprogramowania numerów seryjnych itp. Procedura weryfikacji będzie zależna od możliwości udostępnianych przez producenta oprogramowania.

– **Oprogramowanie antywirusowe:**

1) Rozwiązanie musi wspierać systemy operacyjne Windows (Windows 7/Windows 8/Windows 8.1/Windows 10/Windows 11).
2) Rozwiązanie musi wspierać architekturę ARM64.
3) Rozwiązanie musi zapewniać wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor.
4) Rozwiązanie musi posiadać wbudowaną technologię do ochrony przed rootkitami oraz podłączeniem komputera do sieci botnet.
5) Rozwiązanie musi zapewniać wykrywanie potencjalnie niepożądanych, niebezpiecznych oraz podejrzanych aplikacji
6) Rozwiązanie musi zapewniać skanowanie w czasie rzeczywistym otwieranych, zapisywanych i wykonywanych plików.

7) Rozwiązanie musi zapewniać skanowanie całego dysku, wybranych katalogów lub pojedynczych plików "na żądanie" lub według harmonogramu.
8) Rozwiązanie musi zapewniać skanowanie plików spakowanych i skompresowanych oraz dysków sieciowych i dysków przenośnych.
9) 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.
10) 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).
11) Rozwiązanie musi zapewniać skanowanie ruchu sieciowego wewnątrz szyfrowanych protokołów HTTPS, POP3S, IMAPS.
12) 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.
13) 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.
14) 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.
15) Moduł HIPS musi posiadać możliwość pracy w jednym z pięciu trybów:
    - tryb automatyczny z regułami, gdzie program automatycznie tworzy i wykorzystuje reguły wraz z możliwością wykorzystania reguł utworzonych przez użytkownika,
    - tryb interaktywny, w którym to rozwiązanie pyta użytkownika o akcję w przypadku wykrycia aktywności w systemie,
    - tryb oparty na regułach, gdzie zastosowanie mają jedynie reguły utworzone przez użytkownika,
    - 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,
    - tryb inteligentny, w którym rozwiązanie będzie powiadamiało wyłącznie o szczególnie podejrzanych zdarzeniach.
16) Rozwiązanie musi być wyposażone we wbudowaną funkcję, która wygeneruje pełny raport na temat stacji, na której zostało zainstalowane, w tym przynajmniej z: zainstalowanych aplikacji, usług systemowych, informacji o systemie operacyjnym i sprzęcie, aktywnych procesów i połączeń sieciowych, harmonogramu systemu operacyjnego, pliku hosts, sterowników.
17) 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.
18) Rozwiązanie musi posiadać automatyczną, inkrementacyjną aktualizację silnika detekcji.

19) Rozwiązanie musi posiadać tylko jeden proces uruchamiany w pamięci, z którego korzystają wszystkie funkcje systemu (antywirus, antyspyware, metody heurystyczne).
20) Rozwiązanie musi posiadać funkcjonalność skanera UEFI, który chroni użytkownika poprzez wykrywanie i blokowanie zagrożeń, atakujących jeszcze przed uruchomieniem systemu operacyjnego.

– **Oprogramowanie antywirusowe:**

1) Rozwiązanie musi wspierać systemy operacyjne Windows (Windows 7/Windows 8/Windows 8.1/Windows 10/Windows 11).
2) Rozwiązanie musi wspierać architekturę ARM64.
3) Rozwiązanie musi zapewniać wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor.
4) Rozwiązanie musi posiadać wbudowaną technologię do ochrony przed rootkitami oraz podłączeniem komputera do sieci botnet.
5) Rozwiązanie musi zapewniać wykrywanie potencjalnie niepożądanych, niebezpiecznych oraz podejrzanych aplikacji.
6) Rozwiązanie musi zapewniać skanowanie w czasie rzeczywistym otwieranych, zapisywanych i wykonywanych plików.
7) Rozwiązanie musi zapewniać skanowanie całego dysku, wybranych katalogów lub pojedynczych plików "na żądanie" lub według harmonogramu.
8) Rozwiązanie musi zapewniać skanowanie plików spakowanych i skompresowanych oraz dysków sieciowych i dysków przenośnych.
9) 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.
10) 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).
11) Rozwiązanie musi zapewniać skanowanie ruchu sieciowego wewnątrz szyfrowanych protokołów HTTPS, POP3S, IMAPS.
12) 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.
13) 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.
14) 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.
15) Moduł HIPS musi posiadać możliwość pracy w jednym z pięciu trybów:
    - tryb automatyczny z regułami, gdzie program automatycznie tworzy i wykorzystuje reguły wraz z możliwością wykorzystania reguł utworzonych przez użytkownika,
    - tryb interaktywny, w którym to rozwiązanie pyta użytkownika o akcję w przypadku wykrycia aktywności w systemie,

- tryb oparty na regułach, gdzie zastosowanie mają jedynie reguły utworzone przez użytkownika,
- 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,
- tryb inteligentny, w którym rozwiązanie będzie powiadamiało wyłącznie o szczególnie podejrzanych zdarzeniach.

16) Rozwiązanie musi być wyposażone we wbudowaną funkcję, która wygeneruje pełny raport na temat stacji, na której zostało zainstalowane, w tym przynajmniej z: zainstalowanych aplikacji, usług systemowych, informacji o systemie operacyjnym i sprzęcie, aktywnych procesów i połączeń sieciowych, harmonogramu systemu operacyjnego, pliku hosts, sterowników.
17) 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.
18) Rozwiązanie musi posiadać automatyczną, inkrementacyjną aktualizację silnika detekcji.
19) Rozwiązanie musi posiadać tylko jeden proces uruchamiany w pamięci, z którego korzystają wszystkie funkcje systemu (antywirus, antyspyware, metody heurystyczne).
20) Rozwiązanie musi posiadać funkcjonalność skanera UEFI, który chroni użytkownika poprzez wykrywanie i blokowanie zagrożeń, atakujących jeszcze przed uruchomieniem systemu operacyjnego.

– **Administracja zdalna:**

1) Rozwiązanie musi wspierać instalację na systemach Windows Server (od 2012), Linux oraz w postaci maszyny wirtualnej w formacie OVA lub dysku wirtualnego w formacie VHD.
2) Rozwiązanie musi zapewniać instalację z użyciem nowego lub istniejącego serwera bazy danych MS SQL i MySQL.
3) Rozwiązanie musi zapewniać pobranie wszystkich wymaganych elementów serwera centralnej administracji w postaci jednego pakietu instalacyjnego i każdego z modułów oddzielnie bezpośrednio ze strony producenta.
4) Rozwiązanie musi zapewniać dostęp do konsoli centralnego zarządzania w języku polskim z poziomu interfejsu WWW zabezpieczony za pośrednictwem protokołu SSL.
5) Rozwiązanie musi zapewniać zabezpieczoną komunikację pomiędzy poszczególnymi modułami serwera za pomocą certyfikatów.
6) Rozwiązanie musi zapewniać utworzenia własnego CA (Certification Authority) oraz dowolnej liczby certyfikatów z podziałem na typ elementu: agent, serwer zarządzający, serwer proxy, moduł zarządzania urządzeniami mobilnymi.
7) Rozwiązanie musi wspierać zarządzanie urządzeniami z systemem iOS i Android.
8) Rozwiązanie musi zapewniać centralną konfigurację i zarządzanie przynajmniej takimi modułami jak: ochrona antywirusowa, antyspyware, które działają na stacjach roboczych w sieci.
9) Rozwiązanie musi zapewniać weryfikację podzespołów zarządzanego komputera (w tym przynajmniej: producent, model, numer seryjny, informacje o systemie, procesor, pamięć RAM, wykorzystanie dysku twardego, informacje o wyświetlaczu, urządzenia peryferyjne, urządzenia audio, drukarki, karty sieciowe, urządzenia masowe).

10) Rozwiązanie musi zapewniać instalowanie i odinstalowywanie oprogramowania firm trzecich dla systemów Windows oraz MacOS oraz odinstalowywanie oprogramowania zabezpieczającego firm trzecich, zgodnych z technologią OPSWAT.
11) Rozwiązanie musi zapewniać wymuszenia dwufazowej autoryzacji podczas logowania do konsoli administracyjnej.
12) Serwer administracyjny musi posiadać możliwość tworzenia grup statycznych i dynamicznych komputerów.
13) 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.
14) Rozwiązanie musi zapewniać korzystanie z minimum 100 szablonów raportów, przygotowanych przez producenta oraz musi zapewniać tworzenie własnych raportów przez administratora.
15) Rozwiązanie musi zapewniać wysłanie powiadomienia przynajmniej za pośrednictwem wiadomości email, komunikatu SNMP oraz do dziennika syslog.
16) Rozwiązanie musi zapewniać podział uprawnień administratorów w taki sposób, aby każdy z nich miał możliwość zarządzania konkretnymi grupami komputerów, politykami oraz zadaniami.

– **Ochrona serwera**

1) Rozwiązanie musi wspierać systemy Microsoft Windows Server 2012 i nowszych oraz Linux w tym co najmniej: RedHat Enterprise Linux (RHEL) 7 i 8, CentOS 7 i 8, Ubuntu Server 16.04 LTS i nowsze, Debian 9, Debian 10, SUSE Linux Enterprise Server (SLES) 12, SUSE Linux Enterprise Server (SLES) 15, Oracle Linux oraz Amazon Linux.
2) Rozwiązanie musi zapewniać ochronę przed wirusami, trojanami, robakami i innymi zagrożeniami.
3) Rozwiązanie musi zapewniać wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor.
4) Rozwiązanie musi zapewniać możliwość skanowania dysków sieciowych typu NAS.
5) 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.
6) Rozwiązanie musi wspierać automatyczną, inkrementacyjną aktualizację silnika detekcji.
7) Rozwiązanie musi posiadać możliwość wykluczania ze skanowania procesów.
8) Rozwiązanie musi posiadać możliwość określenia typu podejrzanych plików, jakie będą przesyłane do producenta, w tym co najmniej pliki wykonywalne, archiwa, skrypty, dokumenty.

Dodatkowe wymagania dla ochrony serwerów Windows:

9) Rozwiązanie musi posiadać możliwość skanowania plików i folderów, znajdujących się w usłudze chmurowej OneDrive.
10) Rozwiązanie musi posiadać system zapobiegania włamaniom działający na hoście (HIPS).
11) Rozwiązanie musi wspierać skanowanie magazynu Hyper-V.

12) Rozwiązanie musi posiadać funkcjonalność skanera UEFI, który chroni użytkownika poprzez wykrywanie i blokowanie zagrożeń, atakujących jeszcze przed uruchomieniem systemu operacyjnego.
13) 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.
14) Rozwiązanie musi automatyczne wykrywać usługi zainstalowane na serwerze i tworzyć dla nich odpowiednie wyjątki.
15) Rozwiązanie musi posiadać wbudowany system IDS z detekcją prób ataków, anomalii w pracy sieci oraz wykrywaniem aktywności wirusów sieciowych.
16) Rozwiązanie musi zapewniać możliwość dodawania wyjątków dla systemu IDS, co najmniej w oparciu o występujący alert, kierunek, aplikacje, czynność oraz adres IP.
17) Rozwiązanie musi posiadać ochronę przed oprogramowaniem wymuszającym okup za pomocą dedykowanego modułu.

– **Oprogramowanie biurowe:**

Licencja na pakiet aplikacji biurowych nie może być ograniczona czasowo. Praca na aplikacjach zawartych w pakiecie musi być możliwa także bez połączenia z siecią Internet.
Pakiet biurowy musi spełniać następujące wymagania:

1) Wymagania odnośnie interfejsu użytkownika:
   a) Pełna polska wersja językowa interfejsu użytkownika
   b) Prostota i intuicyjność obsługi, pozwalająca na pracę osobom nieposiadającym umiejętności technicznych
   c) Możliwość zintegrowania uwierzytelniania użytkowników z usługą katalogową (Active Directory lub funkcjonalnie równoważną) – użytkownik raz zalogowany z poziomu systemu operacyjnego stacji roboczej ma być automatycznie rozpoznawany we wszystkich modułach oferowanego rozwiązania bez potrzeby oddzielnego monitowania go o ponowne uwierzytelnienie się.
2) Oprogramowanie musi umożliwiać tworzenie i edycję dokumentów elektronicznych w ustalonym formacie, który spełnia następujące warunki:
   a) posiada kompletny i publicznie dostępny opis formatu,
   b) ma zdefiniowany układ informacji w postaci XML zgodnie z Tabelą B1 załącznika 2 Rozporządzenia w sprawie minimalnych wymagań dla systemów teleinformatycznych (Dz.U.05.212.1766)
   c) umożliwia wykorzystanie schematów XML
   d) wspiera w swojej specyfikacji podpis elektroniczny zgodnie z Tabelą A.1.1 załącznika 2 Rozporządzenia w sprawie minimalnych wymagań dla systemów teleinformatycznych (Dz.U.05.212.1766)
3) Oprogramowanie musi umożliwiać dostosowanie dokumentów i szablonów do potrzeb instytucji oraz udostępniać narzędzia umożliwiające dystrybucję odpowiednich szablonów do właściwych odbiorców.
4) W skład oprogramowania muszą wchodzić narzędzia programistyczne umożliwiające automatyzację pracy i wymianę danych pomiędzy dokumentami i aplikacjami (język makropoleceń, język skryptowy)
5) Do aplikacji musi być dostępna pełna dokumentacja w języku polskim.

6) Pakiet zintegrowanych aplikacji biurowych musi zawierać:
   a) Edytor tekstów
   b) Arkusz kalkulacyjny
   c) Narzędzie do przygotowywania i prowadzenia prezentacji
   d) Narzędzie do zarządzania informacją prywatą (pocztą elektroniczną, kalendarzem, kontaktami i zadaniami)
7) Edytor tekstów musi umożliwiać:
   a) Edycję i formatowanie tekstu w języku polskim wraz z obsługą języka polskiego w zakresie sprawdzania pisowni i poprawności gramatycznej oraz funkcjonalnością słownika wyrazów bliskoznacznych i autokorekty
   b) Wstawianie oraz formatowanie tabel
   c) Wstawianie oraz formatowanie obiektów graficznych
   d) Wstawianie wykresów i tabel z arkusza kalkulacyjnego (wliczając tabele przestawne)
   e) Automatyczne numerowanie rozdziałów, punktów, akapitów, tabel i rysunków
   f) Automatyczne tworzenie spisów treści
   g) Formatowanie nagłówków i stopek stron
   h) Sprawdzanie pisowni w języku polskim
   i) Śledzenie zmian wprowadzonych przez użytkowników
   j) Nagrywanie, tworzenie i edycję makr automatyzujących wykonywanie czynności
   k) Określenie układu strony (pionowa/pozioma)
   l) Wydruk dokumentów
   m) Wykonywanie korespondencji seryjnej bazując na danych adresowych pochodzących z arkusza kalkulacyjnego i z narzędzia do zarządzania informacją prywatną
   n) Pracę na dokumentach utworzonych przy pomocy Microsoft Word 2003 lub Microsoft Word 2007 i 2010 z zapewnieniem bezproblemowej konwersji wszystkich elementów i atrybutów dokumentu
   o) Zabezpieczenie dokumentów hasłem przed odczytem oraz przed wprowadzaniem modyfikacji
   p) Wymagana jest dostępność do oferowanego edytora tekstu bezpłatnych narzędzi umożliwiających wykorzystanie go, jako środowiska udostępniającego formularze bazujące na schematach XML z Centralnego Repozytorium Wzorów Dokumentów Elektronicznych, które po wypełnieniu umożliwiają zapisanie pliku XML w zgodzie z obowiązującym prawem.
   q) Wymagana jest dostępność do oferowanego edytora tekstu bezpłatnych narzędzi (kontrolki) umożliwiających podpisanie podpisem elektronicznym pliku z zapisanym dokumentem przy pomocy certyfikatu kwalifikowanego zgodnie z wymaganiami obowiązującego w Polsce prawa.
   r) Wymagana jest dostępność do oferowanego edytora tekstu bezpłatnych narzędzi umożliwiających wykorzystanie go, jako środowiska udostępniającego formularze i pozwalające zapisać plik wynikowy w zgodzie z Rozporządzeniem o Aktach Normatywnych i Prawnych.
8) Arkusz kalkulacyjny musi umożliwiać:
   a) Tworzenie raportów tabelarycznych
   b) Tworzenie wykresów liniowych (wraz linią trendu), słupkowych, kołowych

c) Tworzenie arkuszy kalkulacyjnych zawierających teksty, dane liczbowe oraz formuły przeprowadzające operacje matematyczne, logiczne, tekstowe, statystyczne oraz operacje na danych finansowych i na miarach czasu.
d) Tworzenie raportów z zewnętrznych źródeł danych (inne arkusze kalkulacyjne, bazy danych zgodne z ODBC, pliki tekstowe, pliki XML, webservice)
e) Obsługę kostek OLAP oraz tworzenie i edycję kwerend bazodanowych i webowych.
f) Narzędzia wspomagające analizę statystyczną i finansową, analizę wariantową i rozwiązywanie problemów optymalizacyjnych
g) Tworzenie raportów tabeli przestawnych umożliwiających dynamiczną zmianę wymiarów oraz wykresów bazujących na danych z tabeli przestawnych
h) Wyszukiwanie i zamianę danych
i) Wykonywanie analiz danych przy użyciu formatowania warunkowego
j) Nazywanie komórek arkusza i odwoływanie się w formułach po takiej nazwie
k) Nagrywanie, tworzenie i edycję makr automatyzujących wykonywanie czynności
l) Formatowanie czasu, daty i wartości finansowych z polskim formatem
m) Zapis wielu arkuszy kalkulacyjnych w jednym pliku.
n) Zachowanie pełnej zgodności z formatami plików utworzonych za pomocą oprogramowania Microsoft Excel 2003 oraz Microsoft Excel 2007 i 2010, z uwzględnieniem poprawnej realizacji użytych w nich funkcji specjalnych i makropoleceń.
o) Zabezpieczenie dokumentów hasłem przed odczytem oraz przed wprowadzaniem modyfikacji

9) Narzędzie do przygotowywania i prowadzenia prezentacji musi umożliwiać:
a) Przygotowywanie prezentacji multimedialnych
b) Prezentowanie przy użyciu projektora multimedialnego
c) Drukowanie w formacie umożliwiającym robienie notatek
d) Zapisanie jako prezentacja tylko do odczytu
e) Nagrywanie narracji i dołączanie jej do prezentacji
f) Opatrywanie slajdów notatkami dla prezentera
g) Umieszczanie i formatowanie tekstów, obiektów graficznych, tabel, nagrań dźwiękowych i wideo
h) Umieszczanie tabel i wykresów pochodzących z arkusza kalkulacyjnego
i) Odświeżenie wykresu znajdującego się w prezentacji po zmianie danych w źródłowym arkuszu kalkulacyjnym
j) Możliwość tworzenia animacji obiektów i całych slajdów
k) Prowadzenie prezentacji w trybie prezentera, gdzie slajdy są widoczne na jednym monitorze lub projektorze, a na drugim widoczne są slajdy i notatki prezentera
l) Pełna zgodność z formatami plików utworzonych za pomocą oprogramowania MS PowerPoint 2003, MS PowerPoint 2007 i 2010.

10) Narzędzie do zarządzania informacją prywatną (pocztą elektroniczną, kalendarzem, kontaktami i zadaniami) musi umożliwiać:
a) Pobieranie i wysyłanie poczty elektronicznej z serwera pocztowego
b) Filtrowanie niechcianej poczty elektronicznej (SPAM) oraz określanie listy zablokowanych i bezpiecznych nadawców
c) Tworzenie katalogów, pozwalających katalogować pocztę elektroniczną
d) Automatyczne grupowanie poczty o tym samym tytule

e) Tworzenie reguł przenoszących automatycznie nową pocztę elektroniczną do określonych katalogów bazując na słowach zawartych w tytule, adresie nadawcy i odbiorcy
f) Oflagowanie poczty elektronicznej z określeniem terminu przypomnienia
g) Zarządzanie kalendarzem
h) Udostępnianie kalendarza innym użytkownikom
i) Przeglądanie kalendarza innych użytkowników
j) Zapraszanie uczestników na spotkanie, co po ich akceptacji powoduje automatyczne wprowadzenie spotkania w ich kalendarzach
k) Zarządzanie listą zadań
l) Zlecanie zadań innym użytkownikom
m) Zarządzanie listą kontaktów
n) Udostępnianie listy kontaktów innym użytkownikom
o) Przeglądanie listy kontaktów innych użytkowników
p) Możliwość przesyłania kontaktów innym użytkowników

5. System bezpieczeństwa logowania

Na system bezpieczeństwa składa się:
1) Uruchomienie usług domenowych dla Urzędu (uruchomienie usługi katalogowej, uruchomienie Infrastruktury klucza prywatnego - PKI, uruchomienie usługi zdalnego pulpitu),
2) Wdrożenie karty pracowniczej (EKP) wraz uruchomieniem systemu bezpiecznego logowania – możliwości uwierzytelniania pracowników w oparciu o kartę pracowniczą,
3) Dostawa kart, uchwytów do kart, smyczy, czytników kart procesorowych wraz z oprogramowaniem.

Wykonawca jest zobowiązany do:
1) Uruchomienia usług domenowych w oparciu o dostarczone licencje oraz dostawę kart wraz z usługą personalizacji kart procesorowych w centrum personalizacji kart Wykonawcy,
2) Uruchomienia uwierzytelniania pracowników w oparciu o dostarczoną kartę procesorową na stanowiskach komputerowych Zamawiającego wyposażonych w czytniki kart,
3) Testy wdrożonych usług katalogowych oraz usług kartowych,
4) Uruchomienie produkcyjne wdrożonych usług oraz karty pracowniczej.
5) Wszystkie usługi zostaną uruchomione w środowisku zwirtualizowanym oraz w oparciu o dostarczone licencje wraz ze sprzętem.
6) Wykonawca docelowo dostarczy elektroniczną kartę pracownika (EKP) zgodnie ze specyfikacją blankietów opisaną w punkcie Wymagania techniczno-funkcjonalne dla karty elektronicznej, a następnie dokona spersonalizowania graficznego oraz elektronicznego blankietów karty pracowniczej dla Zamawiającego we własnym centrum personalizacji kart procesorowych. Dane pracowników zostaną dostarczone przez Zamawiającego zgodnie z wymaganiami Wykonawcy. Dostarczone karty pracownika (EKP) mają wspierać bezpieczne logowanie pracowników do stacji roboczych z wykorzystaniem czytników kart poprzez uwierzytelnianie pracowników na podstawie wgranego certyfikatu PKI na kartę pracowniczą (Wykonawca uruchomi centrum certyfikacji CA w oparciu o usługę infrastruktury klucza prywatnego PKI).

7) Szczegółowe wymagania w zakresie instalacji i konfiguracji zostaną przekazane przez Zamawiającego na etapie wdrażania zaprojektowanych rozwiązań.
8) Wykonawca ponadto przeprowadzi testy uruchomionych usług oraz dostarczonego sprzętu, a także przeszkoli administratora Zamawiającego w zakresie ustalonym przez strony.

Wymagania techniczno-funkcjonalne dla karty elektronicznej – blankietu EKP.

1) **Karta procesorowa Blankiet EKP (Karta)** jest hybrydową elektroniczną kartą procesorową z dwoma interfejsami (dwoma, niezależnymi układami elektronicznymi):
   a) stykowym określonym w normach ISO/IEC 7816-2 i ISO/IEC 7816-3 o pojemności całkowitej pamięci EEPROM co najmniej 390 kilobajtów, w tym dostępnej co najmniej 67 kilobajtów.
   b) bezstykowym określonym w normie ISO/IEC 14443 typ A, zgodnym ze standardem przemysłowym MIFARE® dla protokołu klasycznego o pojemności pamięci 1 kilobajt (MIFARE® Standard Card IC MF1 IC S50 Functional Specification lub równoważny).

Karty wykonane są z materiału nie ulegającemu odkształceniu i / lub rozwarstwieniu.
Blankiet może być stosowany jako kwalifikowane urządzenie do składania podpisu elektronicznego zgodnie z wymogami Rozporządzenia Parlamentu Europejskiego i Rady (UE) NR 910/2014 z dnia 23 lipca 2014 r. w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym oraz uchylające dyrektywę 1999/93/WE – Załącznik II Wymogi dla kwalifikowanych urządzeń do składania podpisu elektronicznego -, na które powołuje się Ustawa z dnia 5 września 2016 r. o usługach zaufania oraz identyfikacji elektronicznej (Dz.U. 2016 poz. 1579, tekst jednolity Dz.U. 2019 poz. 162).

2) Wygląd blankietu

Blankiet powinien umożliwiać nadanie wyglądu EKP określonego przez Zamawiającego.

3) Część elektroniczna – stykowa

Część stykowa karty jest wyposażona w interfejs określony w normach ISO/IEC 7816-2 i ISO/IEC 7816-3.
Polecenia i odpowiedzi przesyłane podczas komunikacji Karty z infrastrukturą informatyczną powinny mieć strukturę zgodną z APDU określoną w normie ISO/IEC 7816-4.
Polecenia realizowane przez Kartę dla operacji kryptograficznych i zarządzania są zgodne z ISO/IEC 7816-8, ISO/IEC 7816-9.

Blankiet EKP musi spełniać następujące wymagania:

- Układ elektroniczny o dostępnej pamięci co najmniej 67 kilobajtów z wbudowanym koprocesorem kryptograficznym.
- Układ elektroniczny blankietu EKP musi posiadać certyfikat Common Criteria Standard na poziomie co najmniej EAL5+.
- Card Management i API zgodne z Global Platform 2.1.1
- System operacyjny Java Card Virtual Machine, RTE i API zgodne z JC2.2.2 wraz z rozszerzeniami JC 3.0.4 o wsparcie dla kryptografii bazującej na krzywych eliptycznych (ECC)
- Blankiet EKP musi posiadać certyfikat Common Criteria Standard na poziomie co najmniej EAL5+ według profilu PP SSCD/QSCD Protection Profile – Qualified Signature Creation Device/Secure Signature Creation Device wg EN 419211 część 1 do 6 (poprzednio publikowane pod kodem EN 14169). Zgodność ze specyfikacją eIDAS.

- Zgodny ze standardem funkcjonalności E-Sign K (CWA14890).
- DAP zgodne z Global Platform 2.1.1 (PK-Based).
- Funkcjonalność PKI zgodna ze standardem minidriver ver. 7.x firmy Microsoft oraz PKCS#11 ver. 2.20. Minidriver dla karty powinien być dostępny na stronach Microsoft Update.
- Obsługiwane protokoły: T=0, T=1, PPS.
- Prędkość transmisji czytnik – karta do 230 Kbauds.
- Dostęp do klucza prywatnego zapisanego na Karcie możliwy jest wyłącznie przez koprocesor kryptograficzny Karty.
- Wszystkie operacje kryptograficzne dotyczące klucza prywatnego wykonywane na karcie.
- Użycie klucza prywatnego tylko po podaniu kodu PIN użytkownika. Osobna para PIN/PUK dla kluczy związanych z kwalifikowanym certyfikatem.
- Blankiet EKP w części stykowej musi pozwalać na zarządzanie pamięcią EEPROM poprzez: usuwanie apletów/pakietów, udostępnianie pamięci zwolnionej po usunięciu apletu/pakietu i defragmentację luk w pamięci EEPROM.
- Generowanie kluczy kryptograficznych o długości do 2048 bitów (opcjonalnie do 4096 bitów) przeznaczonych do użycia przez algorytm RSA, podpisywanie za pomocą algorytmu RSA, generowanie kluczy kryptograficznych ECC o długości do 521 bitów, podpisywanie za pomocą algorytmu ECC, obsługa funkcji skrótu SHA-1, SHA-256, SHA-384, SHA-512, obsługa algorytmów 3DES (ECB, CBC), AES (128, 192, 256 bitów).
- Karta przystosowana do umieszczenia na niej certyfikatu kwalifikowanego wraz z kluczami kryptograficznymi oraz certyfikatu niekwalifikowanego wraz z kluczami kryptograficznymi; certyfikaty mogą zostać umieszczone w późniejszym czasie.

4) Część elektroniczna – bezstykowa

Część bezstykowa jest wyposażona w interfejs zgodny z ISO/IEC 14443 typ A.
Sposób komunikacji karty jest zgodny ze standardem przemysłowym MIFARE® dla protokołu klasycznego spełniającym wymagania normy ISO/IEC 14443-1, ISO/IEC 14443-2, ISO/IEC 14443-3 oraz opcjonalnie ISO/IEC 14443-4 (protokół T=CL), przy zachowaniu pełnej antykolizyjności.

5) Zabezpieczenia na czas dostawy

Dostęp do układów elektronicznych blankietów EKP jest zabezpieczany na czas dostawy specjalnymi kluczami transportowymi dla części bezstykowej (MIFARE®) i stykowej.

Gwarancja na dostarczone elementy min. 24 miesiące

6. Serwer wirtualizacyjny – szt. 2 – wymagania minimalne

– **Obudowa:**

1) Typu Rack, wysokość maksimum 1U;
2) Dostarczona wraz z szynami umożliwiającymi wysunięcie serwera z szafy rack;
3) Minimum 8 wnęk dla dysków Hotplug 2,5 cala,

– **Płyta główna:**

1) Dwuprocesorowa, zaprojektowana i wyprodukowana przez producenta serwera, możliwość instalacji procesorów czterdziestordzeniowych;
2) Wyposażona w minimum 32 gniazda pamięci RAM DDR4;

3) Minimum 3 złącza PCI Express generacji 4 o prędkości x16, w tym min. 2 złącza aktywne w dostarczonej konfiguracji;
4) Minimum 2 sloty dla dysków M.2 na płycie głównej (lub dedykowanej karcie PCI Express) nie zajmujące klatek dla dysków hot-plug; (Możliwość integracji dedykowanej, wewnętrznej pamięci flash przeznaczonej dla wirtualizatora w slocie M.2 bez zajmowania klatek dyskowych serwera);

– **Procesory:**

Zainstalowany 1 procesor max. 8-rdzeniowy w architekturze x86 osiągający w testach wydajności SPECrate2017_int_base minimum 125 pkt w teście dla konfiguracji dwuprocesorowej. Wynik dla oferowanego modelu serwera i o zgodnym modelu procesora/ów musi być dostępny na stronie spec.org na dzień składania ofert. Dopuszczalny jest wynik SPEC dla innego modelu serwera niż oferowany jeśli będzie to wynik dla serwera tego samego producenta, z tej samej linii produktowej, oraz wykorzystującego ten sam chipset co oferowany model serwera;

– **Pamięć RAM:**

1) Zainstalowane 64 GB pamięci RAM typu DDR4 Registered, 3200Mhz w modułach o pojemności 32GB;
2) Oferowany serwer musi zapewniać możliwość rozbudowy/rekonfiguracji pamięci RAM i procesora/ów (dopuszczalna jest konieczność wymiany tych elementów) tak aby zapewnić:
3) Obsługę do 4000GB pamięci RAM DDR4 3200 MHz i do 10000GB pamięci RAM DDR4 i Optane PMem;
4) Obsługę zabezpieczania pamięci: Advanced ECC, Memory Scrubbing, SDDC lub równoważnej;
5) Obsługę kopii lustrzanej pamięci RAM (memory mirror);

Kontrolery dyskowe, I/O

6) Zainstalowany kontroler SAS 3.0 RAID 0,1,5,50 nie zajmujący slotów PCIe serwera opisanych w pkt. „płyta główna” (dopuszcza się instalację w slocie PCI Express pod warunkiem dostarczenia serwera z większą niż wymagana ilości slotów PCI Express);

– **Dyski twarde:**

1) Zainstalowane 2 dyski SSD hot-plug o pojemności 240GB każdy. Dyski dedykowane do pracy w serwerach o parametrze DWPD 1.5 dla okresu 5 lat.
2) Zainstalowane 3 dyski SSD hot-plug o pojemności 960GB każdy. Dyski dedykowane do pracy w serwerach o parametrze DWPD 1.5 dla okresu 5 lat.

Inne napędy zintegrowane:

3) Możliwość rozbudowy serwera o wewnętrzny napęd Blue-ray (odczyt/zapis);

Kontrolery LAN:

4) Karta LAN 2x10Gbit/s SFP+ niezajmująca slotu PCI Express (dopuszcza się instalację w slocie PCI Express pod warunkiem dostarczenia serwera z większą niż wymagana ilości slotów PCI Express);
5) Możliwość rozbudowy serwera do konfiguracji wyposażonej w drugą kartę LAN 4x1Gbit/s / 2x 10Gbit/s RJ-45 / 2x 10Gbit/s SFP+ / 4x10Gbit/s SFP+ / 2 x 25 Gbit/s QSFP28/2 x 100 Gbit/s QSFP28, niezajmująca slotu PCI Express (dopuszcza się możliwość instalacji karty w slocie PCI Express pod warunkiem dostarczenia serwera z większą niż wymagana ilości slotów PCI Express);
6) Zainstalowana dodatkowa karta LAN 4x1GbE RJ-45;

– **Porty:**

1) zintegrowana karta graficzna ze złączem VGA z tyłu serwera;
2) min. 2x USB 3.0 dostępne na froncie obudowy;
3) min. 2x USB 3.0 dostępne z tyłu serwera;
4) min. 1xUSB 3.0 wewnątrz serwera;
5) możliwość rozbudowy o złącze VGA dostępne z przodu serwera;

Ilość dostępnych złącz VGA i USB nie może być osiągnięta poprzez stosowanie zewnętrznych przejściówek, rozgałęziaczy czy dodatkowych kart rozszerzeń zajmujących jakikolwiek slot PCI Express serwera;

– **Zasilanie, chłodzenie:**

1) Redundantne zasilacze hotplug o mocy max. 900W i sprawności 94% (tzw klasa Platinum)
2) Redundantne wentylatory hotplug;

– **Zarządzanie:**

1) Wbudowane diody informacyjne lub wyświetlacz informujące o stanie serwera (system przewidywania, rozpoznawania awarii) – co najmniej informacja o statusie pracy (poprawny/przewidywana usterka lub usterka) następujących komponentów: karty rozszerzeń zainstalowane w dowolnym slocie PCI Express, procesory CPU, pamięć RAM z dokładnością umożliwiającą jednoznaczną identyfikację uszkodzonego modułu pamięci RAM, wbudowany na płycie głównej nośnik pamięci M.2 SSD, status karty zrządzającej serwera, wentylatory, bateria podtrzymująca ustawienia BIOS/Płyty głównej, zasilacze - poprawność napięć elektrycznych płyty głównej w trybie włączonym (on) i oczekiwania (standby) serwera.
2) Zintegrowany z płytą główną serwera kontroler sprzętowy zdalnego zarządzania zgodny z IPMI 2.0 o funkcjonalnościach:
   - Niezależny od systemu operacyjnego, sprzętowy kontroler umożliwiający pełne zarządzanie, zdalny restart serwera;
   - Dedykowana karta LAN 1 Gb/s (dedykowane złącze RJ-45 z tyłu obudowy) do komunikacji wyłącznie z kontrolerem zdalnego zarządzania z możliwością przeniesienia tej komunikacji na inną kartę sieciową współdzieloną z systemem operacyjnym;
   - Dostęp poprzez przeglądarkę Web (także SSL, SSH)
   - Zarządzanie mocą i jej zużyciem oraz monitoring zużycia energii
   - Zarządzanie alarmami (zdarzenia poprzez SNMP)
   - Możliwość przejęcia konsoli tekstowej
   - Przekierowanie konsoli graficznej na poziomie sprzętowym oraz możliwość montowania zdalnych napędów i ich obrazów na poziomie sprzętowym (cyfrowy KVM)
   - Sprzętowy monitoring serwera w tym stanu dysków twardych i kontrolera RAID (bez pośrednictwa agentów systemowych)
   - Możliwe do pobrania oprogramowanie zarządzające i diagnostyczne wyprodukowane przez producenta serwera umożliwiające konfigurację kontrolera RAID, instalację systemów operacyjnych, zdalne zarządzanie, diagnostykę i przewidywanie awarii w oparciu o informacje dostarczane w ramach zintegrowanego w serwerze systemu umożliwiającego monitoring systemu i środowiska (min. temperatura, dyski, zasilacze, płyta główna, procesory, pamięć operacyjna).
   - Dedykowana, wbudowana w kartę zarządzającą pamięć flash o pojemności minimum 16 GB

- Rozwiązanie musi umożliwiać instalację obrazów systemów, własnych narzędzi diagnostycznych w obrębie dostarczonej dedykowanej pamięci (pojemność dostępna dla obrazów własnych – minimum 8,5GB);
- Możliwość zdalnej naprawy systemu operacyjnego uszkodzonego przez użytkownika, działanie wirusów i szkodliwego oprogramowania;
- Możliwość zdalnej reinstalacji systemu lub aplikacji z obrazów zainstalowanych w obrębie dedykowanej pamięci flash bez użytkowania zewnętrznych nośników lub kopiowania danych poprzez sieć LAN;
- Możliwość konfiguracji i wykonania aktualizacji BIOS, Firmware, sterowników serwera bezpośrednio z GUI (graficzny interfejs) karty zarządzającej serwera bez pośrednictwa innych nośników zewnętrznych i wewnętrznych poza obrębem karty zarządzającej (w szczególności bez pendrive, dysków twardych wewn. i zewn., itp.) – możliwość manualnego wykonania aktualizacji jak również możliwość automatyzacji;
- Rozwiązanie musi umożliwiać konfigurację i uruchomienie automatycznego powiadomienia serwisu o zbliżającej się lub istniejącej usterce serwera (co najmniej dyski twarde, zasilacze, pamięć RAM, procesory, wentylatory, kontrolery RAID, karty rozszerzeń);
- Możliwość zapisu i przechowywania informacji i logów o pełnym stanie maszyny, w tym usterki i sytuacje krytyczne w obrębie wbudowanej pamięci karty zarządzającej - dostęp do tych informacji musi być niezależny od stanu włączenia serwera oraz stanu sprzętowego w tym np. usterki elementów poza kartą zarządzającą;
- karta zarządzająca musi umożliwiać konfigurację i uruchomienie automatycznego informowania autoryzowanego serwisu producenta serwera o zaistniałej lub zbliżającej się usterce (wymagana jest możliwość automatycznego otworzenia zgłoszenia serwisowego bezpośrednio w systemie producenta serwera, nie dopuszcza się komunikacji SNMP czy email).

– **Wspierane OS:**

1) Windows 2016, Windows 2019, Windows 2022, Oracle Linux 7.9, Oracle Linux 8.5, RedHat 7.9, RedHat 8, VMWare 6.7u3, VMware 7.0u2

– **Gwarancja:**

1) **Min. 24 miesiące gwarancji** producenta serwera w trybie onsite z gwarantowanym czasem reakcji serwisu w następnym dniu roboczym od zgłoszenia usterki (tzw. NBD Response Time lub NBD Reaction Time) dla zgłoszeń dot. awarii sprzętowych serwera (gwarancja jest kryterium oceny);
2) Wymagana możliwość pobrania informacji np. na stronie producenta oferowanego serwera (lub oświadczenie producenta serwera), iż wymagany w postępowaniu poziom gwarancji i wsparcia na sprzęt i oferowane wraz z nim oprogramowanie dotyczy oferowanego serwera;
3) Usługa pozostawienia dysków u Zamawiającego w przypadku awarii.
4) Dostępność części zamiennych co najmniej przez 5 lat od momentu zakupu serwera;
5) Wymagana jest bezpłatna dostępność poprawek i aktualizacji BIOS/Firmware/sterowników dożywotnio dla oferowanego serwera – jeżeli funkcjonalność ta wymaga dodatkowego serwisu lub licencji producenta serwera takowa licencja musi być uwzględniona w ofercie;
6) Wymagana możliwość automatycznego powiadamiania o awarii serwera centrum serwisowego producenta. Jeżeli funkcja taka jest płatna należy ten koszt uwzględnić w ofercie

– **Dokumentacja, inne:**

1) Elementy, z których zbudowane są serwery muszą być produktami producenta tych serwerów lub być przez niego certyfikowane oraz całe muszą być objęte gwarancją producenta, o wymaganym w specyfikacji poziomie SLA (wymagane oświadczenie producenta serwera potwierdzające spełnienie wymagań dołączone wraz z dostawą serwera).
2) Serwer musi być fabrycznie nowy i pochodzić z oficjalnego kanału dystrybucyjnego w Polsce
3) Wymagane oświadczenie producenta serwera dołączone wraz z dostawą serwera, że oferowany do przetargu sprzęt spełnia ten wymóg;
4) Oferent zobowiązany jest dostarczyć wraz z dostawą kartę produktową oferowanego serwera umożliwiającą weryfikację parametrów oferowanego sprzętu w języku polskim lub angielskim;
5) Ogólnopolska, telefoniczna linia techniczna producenta serwera (ogólnopolski numer stacjonarny lub o zredukowanej odpłatności 0-800/0-801, wraz z dostawą należy podać nr telefonu) umożliwiająca w czasie obowiązywania gwarancji na sprzęt po podaniu numeru seryjnego urządzenia: zgłoszenie usterki sprzętowej urządzenia oraz weryfikację: konfiguracji sprzętowej serwera, w tym model i typ dysków twardych, procesora, ilość fabrycznie zainstalowanej pamięci operacyjnej, czasu obowiązywania i typ udzielonej gwarancji – obsługa w języku polskim, w trybie całodobowym również w dni świąteczne;
6) Wszystkie parametry i funkcje oferowanego serwera muszą być wspierane przez producenta i zaimplementowane fabrycznie oraz dostępne w seryjnej produkcji danego modelu urządzenia;
   Zamawiający nie dopuszcza dostosowywania funkcji na potrzeby niniejszego postępowania.
7) Wszystkie parametry i funkcje oferowanego serwera muszą być potwierdzone w ogólnodostępnej dokumentacji producenta;
8) Instalacja i konfiguracja według wymagań Zamawiającego, w szczególności:
   - Instalacja dostarczanego sprzętu w szafie zamawiającego, podłączenie redundantne do zasilania
9) Upgrade firmware do najnowszej rekomendowanej przez producenta do posiadanego sprzętu
10) Rejestracja licencji i wsparcia dla sprzętu i oprogramowania
11) Instalacja wirtualizatorora na maszynach fizycznych
12) Konfiguracja środowiska wirtualizacyjnego
13) Uruchomienie maszyn wirtualnych
14) Instalacja i konfiguracja dostarczonego oprogramowania
15) Migracja danych na nowo dostarczone serwery. Do obowiązku wykonawcy należy przeniesienie do środowiska wirtualnego (konwersja na maszyny wirtualne) systemów pracujących w środowisku Zamawiającego:
    - systemu finansowo księgowego Infosytem ERP
    - systemu Płatnik
    - programu kadrowo - płacowego BUK Softres
    - systemu gospodarki odpadami GOMIG
    - systemu bankowego

Wynikiem prac końcowych mają być gotowe do pracy systemy wraz z dotychczas zgromadzonymi w nich danymi.

16) Konfiguracja bakupu na urządzenie Serwer NAS
17) Rekonfiguracja zasobów maszyn wirtualnych
18) Dokumentacja powdrożeniowa z wykonanych prac

7. Zasilacz awaryjny – szt. 1 - wymagania minimalne

- Moc pozorna min. 1500 VA
- Moc rzeczywista min. 1500 W
- Topologia (klasyfikacja IEC 62040-3) Line-interactive z AVR
- Czas przełączenia na baterię max. 4 ms
- Liczba, typ gniazd wyjściowych min. 8 x IEC C13
- Typ gniazda wejściowego IEC C14 10A
- Czas podtrzymania dla 100% obciążenia dla pf=1 min. 5 min
- Czas podtrzymania przy 50% obciążenia dla pf=1 min. 14 min
- Dodatkowe baterie: możliwość dodania min. 4 dodatkowych modułów baterii w celu wydłużenia czasu podtrzymania do 95 minut dla 100% obciążenia przy pf=1
- Kształt napięcia Sinusoidalny
- Baterie wymieniane przez użytkownika "na gorąco"
- Ochrona przed przeładowaniem, głębokim rozładowaniem
- System zarządzania pracą baterii
- Zdolność zwarciowa 45 A w czasie 80 ms
- Możliwość uruchomienia bez napięcia w sieci
- Baterie wewnętrzne o pojemności nie mniejszej niż 9Ah 12V, minimum 4 szt.
- Czas ładowania baterii do poziomu 90% < 3 godz. do 90% pojemności użytkowej
- Interfejs komunikacyjny min. USB, RS232 DB-9 żeński (HID)
- Panel sterowania z wyświetlaczem LCD dostarcza informacji min. o : stanie pracy urządzenia, stanie obciążenia, pomiarach i ustawieniach.
- Sygnały akustyczne min.:
  - Awaria, Niski stan naładowania baterii, Przeciążenie, Serwis
  - Możliwość montażu ręcznego bypassu serwisowego

Gwarancja producenta min. 36 miesięcy dla elektroniki oraz baterii

8. Licencje serwerowego systemu operacyjnego – szt. 1 – wymagania minimalne

Oprogramowanie musi zostać dostarczone dla oferowanych serwerów fizycznych. Oprogramowanie musi być w najnowszej dostępnej wersji. Licencjonowanie zgodnie z wymaganiami producenta oprogramowania.
Licencja na serwerowy system operacyjny musi uprawniać do uruchamiania serwerowego systemu operacyjnego w środowisku fizycznym oraz wirtualnych środowisk serwerowego systemu operacyjnego.
Serwerowy system operacyjny musi posiadać następujące, wbudowane cechy:

1) Możliwość wykorzystania 320 logicznych procesorów oraz co najmniej 4 TB pamięci RAM w środowisku fizycznym.
2) Możliwość wykorzystywania 64 procesorów wirtualnych oraz 1TB pamięci RAM i dysku o pojemności do 64TB przez każdy wirtualny serwerowy system operacyjny.
3) Możliwość budowania klastrów składających się z 64 węzłów, z możliwością uruchamiania 7000 maszyn wirtualnych.
4) Możliwość migracji maszyn wirtualnych bez zatrzymywania ich pracy między fizycznymi serwerami z uruchomionym mechanizmem wirtualizacji (hypervisor) przez sieć Ethernet, bez konieczności stosowania dodatkowych mechanizmów współdzielenia pamięci.
5) Wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany pamięci RAM bez przerywania pracy.
6) Wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany procesorów bez przerywania pracy.
7) Automatyczna weryfikacja cyfrowych sygnatur sterowników w celu sprawdzenia, czy sterownik przeszedł testy jakości przeprowadzone przez producenta systemu operacyjnego.
8) Możliwość dynamicznego obniżania poboru energii przez rdzenie procesorów niewykorzystywane w bieżącej pracy. Mechanizm ten musi uwzględniać specyfikę procesorów wyposażonych w mechanizmy Hyper-Threading.
9) Wbudowane wsparcie instalacji i pracy na wolumenach, które:
   a) pozwalają na zmianę rozmiaru w czasie pracy systemu,
   b) umożliwiają tworzenie w czasie pracy systemu migawek, dających użytkownikom końcowym (lokalnym i sieciowym) prosty wgląd w poprzednie wersje plików i folderów,
   c) umożliwiają kompresję "w locie" dla wybranych plików i/lub folderów,
   d) umożliwiają zdefiniowanie list kontroli dostępu (ACL).
10) Wbudowany mechanizm klasyfikowania i indeksowania plików (dokumentów) w oparciu o ich zawartość.
11) Wbudowane szyfrowanie dysków przy pomocy mechanizmów posiadających certyfikat FIPS 140-2 lub równoważny wydany przez NIST lub inną agendę rządową zajmującą się bezpieczeństwem informacji.
12) Możliwość uruchamianie aplikacji internetowych wykorzystujących technologię ASP.NET
13) Możliwość dystrybucji ruchu sieciowego HTTP pomiędzy kilka serwerów.
14) Wbudowana zapora internetowa (firewall) z obsługą definiowanych reguł dla ochrony połączeń internetowych i intranetowych.
15) Dostępne dwa rodzaje graficznego interfejsu użytkownika:
   a) Klasyczny, umożliwiający obsługę przy pomocy klawiatury i myszy,
   b) Dotykowy umożliwiający sterowanie dotykiem na monitorach dotykowych.
16) Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, przeglądarka internetowa, pomoc, komunikaty systemowe,
17) Możliwość zmiany języka interfejsu po zainstalowaniu systemu, dla co najmniej 10 języków poprzez wybór z listy dostępnych lokalizacji.
18) Mechanizmy logowania w oparciu o:
   a) Login i hasło,
   b) Karty z certyfikatami (smartcard),
   c) Wirtualne karty (logowanie w oparciu o certyfikat chroniony poprzez moduł TPM),

19) Możliwość wymuszania wieloelementowej dynamicznej kontroli dostępu dla: określonych grup użytkowników, zastosowanej klasyfikacji danych, centralnych polityk dostępu w sieci, centralnych polityk audytowych oraz narzuconych dla grup użytkowników praw do wykorzystywania szyfrowanych danych.
20) Wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug&Play).
21) Możliwość zdalnej konfiguracji, administrowania oraz aktualizowania systemu.
22) Dostępność bezpłatnych narzędzi producenta systemu umożliwiających badanie i wdrażanie zdefiniowanego zestawu polityk bezpieczeństwa.
23) Pochodzący od producenta systemu serwis zarządzania polityką dostępu do informacji w dokumentach (Digital Rights Management).
24) Wsparcie dla środowisk Java i .NET Framework 4.x – możliwość uruchomienia aplikacji działających we wskazanych środowiskach.
25) Możliwość implementacji następujących funkcjonalności bez potrzeby instalowania dodatkowych produktów (oprogramowania) innych producentów wymagających dodatkowych licencji:
    a) Podstawowe usługi sieciowe: DHCP oraz DNS wspierający DNSSEC,
    b) Usługi katalogowe oparte o LDAP i pozwalające na uwierzytelnianie użytkowników stacji roboczych, bez konieczności instalowania dodatkowego oprogramowania na tych stacjach, pozwalające na zarządzanie zasobami w sieci (użytkownicy, komputery, drukarki, udziały sieciowe), z możliwością wykorzystania następujących funkcji:
    - Podłączenie do domeny w trybie offline – bez dostępnego połączenia sieciowego z domeną,
    - Ustanawianie praw dostępu do zasobów domeny na bazie sposobu logowania użytkownika na przykład typu certyfikatu użytego do logowania,
    - Odzyskiwanie przypadkowo skasowanych obiektów usługi katalogowej z mechanizmu kosza.
    - Bezpieczny mechanizm dołączania do domeny uprawnionych użytkowników prywatnych urządzeń mobilnych opartych o iOS i Windows 8.1.
    c) Zdalna dystrybucja oprogramowania na stacje robocze.
    d) Praca zdalna na serwerze z wykorzystaniem terminala (cienkiego klienta) lub odpowiednio skonfigurowanej stacji roboczej
    e) Centrum Certyfikatów (CA), obsługa klucza publicznego i prywatnego) umożliwiające:
    - Dystrybucję certyfikatów poprzez http
    - Konsolidację CA dla wielu lasów domeny,
    - Automatyczne rejestrowania certyfikatów pomiędzy różnymi lasami domen,
    - Automatyczne występowanie i używanie (wystawianie) certyfikatów PKI X.509.
    f) Szyfrowanie plików i folderów.
    g) Szyfrowanie połączeń sieciowych pomiędzy serwerami oraz serwerami i stacjami roboczymi (IPSec).
    h) Możliwość tworzenia systemów wysokiej dostępności (klastry typu fail-over) oraz rozłożenia obciążenia serwerów.
    i) Serwis udostępniania stron WWW.
    j) Wsparcie dla protokołu IP w wersji 6 (IPv6),
    k) Wsparcie dla algorytmów Suite B (RFC 4869),

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

m) Wbudowane mechanizmy wirtualizacji (Hypervisor) pozwalające na uruchamianie do 1000 aktywnych środowisk wirtualnych systemów operacyjnych. Wirtualne maszyny w trakcie pracy i bez zauważalnego zmniejszenia ich dostępności mogą być przenoszone pomiędzy serwerami klastra typu failover z jednoczesnym zachowaniem pozostałej funkcjonalności. Mechanizmy wirtualizacji mają zapewnić wsparcie dla:

- Dynamicznego podłączania zasobów dyskowych typu hot-plug do maszyn wirtualnych,
- Obsługi ramek typu jumbo frames dla maszyn wirtualnych.
- Obsługi 4-KB sektorów dysków
- Nielimitowanej liczby jednocześnie przenoszonych maszyn wirtualnych pomiędzy węzłami klastra
- Możliwości wirtualizacji sieci z zastosowaniem przełącznika, którego funkcjonalność może być rozszerzana jednocześnie poprzez oprogramowanie kilku innych dostawców poprzez otwarty interfejs API.
- Możliwości kierowania ruchu sieciowego z wielu sieci VLAN bezpośrednio do pojedynczej karty sieciowej maszyny wirtualnej (tzw. trunk mode)

26) Możliwość automatycznej aktualizacji w oparciu o poprawki publikowane przez producenta wraz z dostępnością bezpłatnego rozwiązania producenta serwerowego systemu operacyjnego umożliwiającego lokalną dystrybucję poprawek zatwierdzonych przez administratora, bez połączenia z siecią Internet.
27) Wsparcie dostępu do zasobu dyskowego poprzez wiele ścieżek (Multipath).
28) Możliwość instalacji poprawek poprzez wgranie ich do obrazu instalacyjnego.
29) Mechanizmy zdalnej administracji oraz mechanizmy (również działające zdalnie) administracji przez skrypty.
30) Możliwość zarządzania przez wbudowane mechanizmy zgodne ze standardami WBEM oraz WS-Management organizacji DMTF.
31) Wymaga się aby oferowana licencja umożliwiała korzystanie przez min. 23 użytkowników oraz umożliwiała korzystanie przez zdalny dostęp przez min. 5 użytkowników.
32) Szczegółowe wymagania w zakresie instalacji i konfiguracji zostaną przekazane przez Zamawiającego na etapie wdrażania zaprojektowanych rozwiązań.

9. Licencja bezpieczeństwa danych – szt.1 – wymagania minimalne

1) Oprogramowanie musi zostać dostarczone do oferowanego serwera fizycznego.
2) Oprogramowanie musi być dostarczone w najnowszej dostępnej w dniu dostawy wersji.
3) Rozwiązanie musi zapewniać wsparcie backupu dla następujących platform wirtualizacyjnych, środowisk chmurowych i maszyn fizycznych, przy czym obsługa poszczególnych z nich może być uwarunkowana wybranym typem licencji:
   - Microsoft Server z rolą Hyper-V min. w wersjach 2022, 2019, 2016, 2012R2, 2012
   - Vmware vSphere min. w wersjach v5.5-7.0.3
   - Nutanix AHV 5.10, 5.15, 5.20 (LTS)
4) Maszyny fizyczne: Windows Server 2022, 2019, 2016, 2012R2, 2012, 2008R2

5) Microsoft 365 (Exchange online, One Drive for Business, Sharepoint)
6) Oprogramowanie musi wspierać wszystkie systemy operacyjne gościa, które są obsługiwane przez natywny backup środowisk VMware vSphere, MS Hyper-V
7) Oprogramowanie musi być niezależne sprzętowo i posiadać możliwość uruchomienia:
   - na serwerze Windows lub Linux
   - jako maszyna wirtualna Vmware
   - jako maszyna wirtualna Amazon
   - na serwerze NAS: ASUSTOR, NETGEAR, QNAP, Synology i Western Digital
8) Oprogramowanie do backupu musi pozwalać na wykorzystanie dowolnego serwera oraz przestrzeni dyskowej (nie dedykowanych), za pośrednictwem protokołów CIFS lub NFS
9) Oprogramowanie nie może wymagać instalacji dedykowanego agenta wewnątrz maszyny wirtualnej w celach backupu/przywracania
10) Oprogramowanie nie może wymagać dodatkowej instalacji zewnętrznych aplikacji lub baz danych (jeżeli oprogramowanie wymaga bazy danych musi ona być instalowana automatycznie z paczki opracowanej przez producenta i nie wymagać dodatkowych licencji).
11) Oprogramowanie należy dostarczyć wraz z wsparciem producenta na okres min. 24 miesięcy

10. Serwer NAS – szt. 1 - wymagania minimalne

Pamięć systemowa min. 2 GB (możliwość rozbudowy do 16GB)
Pamięć flash min. 512MB
Wnęka dysków min. 4 dyski SATA (zainstalowane 4 dyski o pojemności min. 8 TB)
Porty sieciowe min. 2 x 10/100/1000/2500 Mbit/s, 2 x 10Gbit/s SFP+
Port USB min. 4 x 3.2 Gen 1 lub nowszy
Obsługa dysków hot-swap
Montaż w szafie RACK
Obsługa przyspieszenia pamięci podręcznej SSD
Wake on Lan
Poziomy RAID: min. 0, 1, 10 (1+0), 5, 50 (5+0), 6, 60 (6+0),JBOD
Gwarancja min. 36 miesięcy

11. Przełącznik sieciowy – szt. 2 – wymagania minimalne

Porty: min. 48 portów RJ45 min. 10/100/1000Mb/s
Obsługiwane standardy i protokoły: min. IEEE 802.3i, IEEE 802.3u, IEEE 802.3ab, IEEE 802.3x
Automatyczna negocjacja szybkości połączeń
Montaż w szafie rack
Wydajność przełączania min. 90GB/s
Tablica adresów MAC min. 16k
Rozmiar bufora min. 12Mb
Architektura przełączania Store and Forward

Wraz z przełącznikiem należy dostarczyć elementy montażowe do szafy rack 19"
Gwarancja min. 36 miesięcy

12. Szkolenie – szt. 1 – wymagania minimalne

W ramach dostawy sprzętu i oprogramowania należy przeprowadzić szkolenie w siedzibie Zamawiającego w zakresie konfiguracji i obsługi dostarczanych urządzeń i oprogramowania w wymiarze min. 8 godzin dla administratorów systemów wskazanych przez Zamawiającego.
Szkolenie swym zakresem musi w stopniu minimalnym obejmować wykonaną konfigurację sprzętu i oprogramowania rozwiązań objętych zakresem wdrożenia.