**OPZ – Opis przedmiotu zamówienia**

**CZĘŚĆ I ZAMÓWIENIA** **– Rozbudowa posiadanych serwerów o dedykowane dyski**

* + **Przedmiot zamówienia**

Zamówienie dotyczy dostawy dedykowanych przez producenta dysków SSD SAS, ich zainstalowania oraz skonfigurowania RAID 5 w dwóch serwerach Lenovo SR650 V2 MT-M: 7Z73 CTO1WW.

* + **Specyfikacja serwerów**

Serwery, w których mają zostać zainstalowane dyski SSD SAS:

* Typ serwera: Lenovo SR650 V2 MT-M: 7Z73 CTO1WW
* Numery seryjne serwerów:
  + SN: J700NB46
  + SN: J700LWW0
  + **Wymagania dotyczące dysków SSD**
* Typ dysków: SSD SAS (Solid State Drive)
* Producent: Dyski muszą pochodzić od dedykowanego producenta, zgodne z wymaganiami serwera Lenovo SR650 V2
* Ilość dysków: Liczba dysków w konfiguracji RAID 5, zależna od pojemności finalnej nie więcej jak 3 sztuki.
* Pojemność: Całkowita pojemność przy skonfigurowanym RAID 5 na każdym z serwerów powinna wynosić 3,6TB powierzchni netto dostępnej do wykorzystania.
* Szybkość transferu: Dyski SSD SAS muszą charakteryzować się wysoką prędkością odczytu   
  i zapisu, zgodną z wymaganiami dla serwerów klasy enterprise.
* Zgodność: Dyski muszą być w pełni kompatybilne z serwerami Lenovo SR650 V2.
  + **Instalacja i konfiguracja RAID**
* Typ konfiguracji RAID: RAID 5
* Instalacja dysków SSD w serwerach: Dyski SSD muszą zostać zainstalowane w odpowiednich slotach w serwerach Lenovo SR650 V2
* Konfiguracja RAID 5: Konfiguracja RAID 5 ma zapewniać optymalną wydajność oraz redundancję danych, z powierzchnią netto 3,6TB na każdym serwerze.
* Weryfikacja konfiguracji: Po zainstalowaniu dysków oraz skonfigurowaniu macierzy RAID, wykonawca zobowiązany jest do przeprowadzenia testów wydajnościowych oraz weryfikacji poprawności konfiguracji.
  + **Wymagania techniczne**
* Dyski muszą spełniać standardy jakości oraz wydajności producenta, pochodzić z autoryzowanego kanału producenta serwera.
* Konfiguracja RAID musi być przeprowadzona zgodnie z najlepszymi praktykami w zakresie ochrony danych oraz wydajności systemu.
* Wykonawca ma obowiązek dostarczenia dokumentacji technicznej dotyczącej zamontowanych dysków oraz konfiguracji RAID, w tym raportu z testów po zakończeniu instalacji i konfiguracji.
  + **Wymagania dotyczące gwarancji**
* Wykonawca zapewnia gwarancję na dostarczone dyski SSD oraz wykonaną konfigurację RAID na okres co najmniej 24 miesięcy.
* W przypadku uszkodzenia dysku twardego w trakcie trwania gwarancji, dysk pozostaje   
  w posiadaniu Zamawiającego. Wykonawca zobowiązuje się do wymiany uszkodzonego dysku na nowy lub równoważny w jak najkrótszym możliwym czasie, nie przekraczającym 5 dni roboczych od zgłoszenia usterki.
* Wykonawca pokrywa wszelkie koszty związane z wymianą uszkodzonego dysku (koszt zakupu, transport, itp.).
* W przypadku wymiany dysku, wykonawca zobowiązany jest do dokonania ponownej konfiguracji RAID oraz testowania poprawności działania nowego dysku w systemie.

**CZĘŚĆ II – Dostawa UTM dla UG sztuk 1**

System bezpieczeństwa realizuje wszystkie wymienione poniżej funkcje sieciowe i bezpieczeństwa niezależnie od dostawcy łącza. Poszczególne elementy wchodzące w skład systemu bezpieczeństwa mogą być zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub komercyjnych aplikacji instalowanych na platformach ogólnego przeznaczenia. W przypadku implementacji programowej muszą być zapewnione niezbędne platformy sprzętowe wraz z odpowiednio zabezpieczonym systemem operacyjnym.

System realizujący funkcję Firewall zapewnia pracę w jednym z trzech trybów: Routera z funkcją NAT oraz transparentnym.

System wspiera protokoły IPv4 oraz IPv6 w zakresie:

* Firewall.
* Ochrony w warstwie aplikacji.
* Protokołów routingu.

# Urządzenie i licencje

W ramach postępowania powinno zostać dostarczone urządzenie fizyczne i licencje upoważniające do korzystania z aktualnych baz funkcji ochronnych producenta i serwisów **do 30 czerwca 2026 r**.

Zakres wsparcia **do 30 czerwca 2026 r.** musi obejmować:

NGFW + IPS, IPSec + SSL VPN, Audyt Podatności, Antywirus - Zaawansowany AV, Filtr URL –   
min. 70 kategorii, Antyspam.

|  |
| --- |
| ***System UTM*** |
| **Wymagania ogólne** |
| Rozwiązanie musi być dostarczone w postaci komercyjnej platformy sprzętowej  z zabezpieczonym systemem operacyjnym. |
| **Interfejsy** |
| minimum 8 interfejsów 2,5GbE Base-T |
| minimum 1 interfejs 1 GbE SFP |
| Możliwość tworzenia minimum 120 interfejsów wirtualnych definiowanych jako VLANy w oparciu o standard 802.1q. |
| **Zasilanie** |
| Redundantny zasilacz o mocy dopasowanej do samodzielnego zapewnienia zasilania urządzenia, pracujące w sieci 230V 50/60Hz. |
| **Funkcje bezpieczeństwa** |
| System ochrony musi realizować wszystkie z poniższych funkcjonalności. Poszczególne funkcjonalności systemu bezpieczeństwa mogą być realizowane w postaci osobnych platform sprzętowych lub programowych:   * kontrola dostępu – zapora ogniowa klasy StatefulInspection; * kontrola stron Internetowych – Web Filter [WF]; * kontrola zawartości poczty – antyspam [AS] (dla protokołów SMTP, POP3); * kontrola pasma oraz ruchu [QoS i Trafficshaping]; * kontrola aplikacji oraz rozpoznawanie ruchu P2P * ochrona przed wirusami – antywirus [AV] (dla protokołów SMTP, POP3, HTTP, FTP, HTTPS). Skanowanie AV dla plików typu: rar, zip; * ochrona przed atakami - IntrusionPrevention System [IPS/IDS]; * poufność danych - IPSec VPN oraz SSL VPN; * analiza ruchu szyfrowanego protokołem SSL; * ochrona przed zagrożeniami ukierunkowanymi oraz ransomware. |
| **Firewall** |
| Urządzenie ma być wyposażone w Firewall klasy StatefulInspection. |
| Obsługa translacji NAT oraz PAT. |
| Ochrona przed atakami DoS oraz DDoS (floodprotection). |
| Ochrona przed skanowaniem portów. |
| Blokowanie ruchu na podstawie kraju pochodzenia (geolokalizacja IP). |
| Filtrowanie na poziomie warstwy 2 modelu OSI tj. na podstawie adresów MAC. |
| Możliwość ustawienia trybu pracy jako router warstwy trzeciej, jako bridge warstwy drugiej oraz hybrydowo (częściowo jako router, a częściowo jako bridge). |
| Możliwość uwierzytelnienia i autoryzacji użytkowników w oparciu o bazę LDAP (wewnętrzną oraz zewnętrzną), zewnętrzny serwer RADIUS, zewnętrzny serwer Kerberos. |
| Musi posiadać wbudowany analizator reguł, który wskazuje błędy i sprzeczności  w konfiguracji reguł. |
| Możliwość tworzenia wydzielonych stref bezpieczeństwa Firewall np. DMZ. |
| **VPN** |
| Tworzenie połączeń w topologii Site-to-site oraz możliwość definiowania połączeń Client-to-site. |
| Wsparcie sieci VPN typu, minimum: PPTP VPN, IPSec VPN, SSL VPN. |
| Klient VPN producenta rozwiązania współpracujący z dostarczonym rozwiązaniem. |
| Monitorowanie stanu tuneli VPN i stałego utrzymywania ich aktywności. |
| Możliwość przełączania tunelu na łącze zapasowe na wypadek awarii łącza dostawcy podstawowego (VPN Failover). |
| Praca w topologii Hub and Spoke oraz Mesh lub równoważnej. |
| Obsługa mechanizmów minimum IPSec NAT Traversal, DPD, Xauth. |
| Obsługa SSL VPN w trybach portal oraz tunel. |
| **IPS** |
| Wykrywanie włamań oraz anomalii w ruchu sieciowym przy pomocy analizy protokołów, analizy heurystycznej oraz analizy w oparciu o sygnatury kontekstowe. |
| Usuwanie szkodliwej zawartość w kodzie HTML oraz JavaScript żądanej przez użytkownika strony internetowej bez blokowania dostępu do tej strony po usunięciu zagrożenia. |
| Baza wykrywanych ataków musi zawierać co najmniej 1000 wpisów. |
| Wykrywanie anomalii protokołów i ruchu stanowiących podstawową ochronę przed atakami typu DoS oraz DDoS. |
| **Antywirus** |
| Silnik antywirusowy musi zapewniać skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021). |
| Możliwość pracy w trybie przezroczystego serwera poczty (Transparent Email Proxy). |
| Automatyczna aktualizacja sygnatur zagrożeń. |
| Ochrona przed spamem i szkodliwym oprogramowaniem w trakcie transakcji SMTP. |
| Inspekcja komunikacji email realizowanej przy użyciu protokołów SMTP, SMTPS, POP3, POP3S. |
| Wykrywanie, blokowanie i skanowanie załączników poczty email. |
| Tworzenie białych i czarnych list adresów email. |
| Wykrywanie spamu niezależnie od stosowanego języka. |
| Musi korzystać minimum z dwóch różnych serwerów publikujących listy RBL. |
| **Filtr stron WWW** |
| Wbudowany filtr URL oparty o technologię w chmurze, obsługujący minimum 65 kategorii  z możliwością tworzenia własnych kategorii. |
| Filtr URL musi mieć możliwość korzystania z adresów WWW dostępnych w chmurze. |
| Musi udostępniać kategorie minimum spam, hacking, malware, botnets. |
| Baza filtra WWW musi umożliwiać grupowanie w kategorie tematyczne. |
| Filtrowanie treści oraz szkodliwego oprogramowania w obrębie protokołów HTTP i HTTPS. |
| Możliwość blokowania i wysyłania treści poprzez HTTP i HTTPS. |
| Inspekcja z obsługą protokołu TLS 1.3. |
| Filtrowanie plików na podstawie MIME. |
| **Kontrola Aplikacji** |
| Kontrola ruchu na podstawie głębokiej analizy pakietów, nie bazującej jedynie  na wartościach portów TCP/UDP. |
| Wykrywanie i kontrolę mikroaplikacji (np. Gry portalu Facebook). |
| Identyfikacja aplikacji niezależnie od wykorzystywanego portu, protokołu, szyfrowania. |
| **Obsługa Routingu** |
| Obsługa Policy Routingu, routing statyczny i dynamiczny w oparciu o  protokoły minimum: RIPv2, OSPF, BGP. |
| Możliwość realizacji routingu statycznego w oparciu o polityki automatycznego wyboru łącza w trybie failover. |
| Trasowanie pakietów z poziomu wybranej reguły firewall (Policy Based Routing). |
| Trasowanie połączeń IPv6 co najmniej w zakresie trasowania statycznego oraz mechanizmu przełączenia na łącze zapasowe w przypadku awarii łącza podstawowego. |
| Możliwość agregowania linków fizycznych w oparciu o IEEE 802.3ad (LACP). |
| Możliwość wykorzystania mechanizmu SD-WAN poprzez analizę stanu łącza w czasie rzeczywistym i dynamicznym wyborze najkorzystniejszego łącza. |
| **Wydajność** |
| Wydajność systemu Firewall minimum 8 Gbps. |
| Wydajność ochrony przed atakami (IPS) minimum 4 Gbps. |
| Wydajność VPN IPSec minimum 2 Gbps. |
| Minimalna liczba jednoczesnych połączeń: 300 000. |
| Minimum 25.000 nowych połączeń na sekundę. |
| **Bezpieczeństwo** |
| Uwierzytelnianie tożsamości użytkowników za pomocą haseł statycznych i definicji użytkowników przechowywanych w lokalnej bazie systemu. |
| Uwierzytelnianie tożsamości użytkowników za pomocą haseł statycznych i definicji użytkowników przechowywanych w bazach zgodnych z LDAP. |
| Uwierzytelnianie tożsamości użytkowników za pomocą haseł dynamicznych (RADIUS)  w oparciu o zewnętrzne bazy danych. |
| Możliwość budowy architektury uwierzytelniania typu Single Sign On w środowisku Active Directory bez konieczności instalowania jakiegokolwiek oprogramowania na kontrolerze domeny. |
| Polityka bezpieczeństwa systemu zabezpieczeń musi uwzględniać adresy IP, interfejsy, protokoły, usługi sieciowe, użytkowników, reakcje zabezpieczeń, rejestrowanie zdarzeń oraz zarządzanie pasmem sieci (m.in. pasmo gwarantowane i maksymalne, priorytety). |
| **Aktualizacja** |
| Automatyczne ściąganie sygnatur ataków, aplikacji, szczepionek antywirusowych oraz ciągły dostęp do globalnej bazy zasilającej filtr URL. |
| **Zarządzanie** |
| Elementy systemu muszą zapewniać lokalne zarządzanie (HTTPS, SSH) jak i współpracować z dedykowanymi platformami do centralnego zarządzania i monitorowania. |
| Komunikacja systemów zabezpieczeń z platformami zarządzania musi być realizowana  z wykorzystaniem szyfrowanych protokołów. |
| Interfejs administracyjny musi umożliwiać generowanie skryptów z czynności wykonywanych przez administratora. |
| Interfejs administracyjny musi oferować narzędzia do przechwytywania pakietów, wyświetlania otwartych połączeń sieciowych. |
| Możliwość eksportowania logów na zewnętrzny serwer (syslog) z wykorzystaniem transmisji nieszyfrowanej jak i szyfrowanej (TLS). |
| **Certyfikaty i Deklaracje** |
| Element oferowanego systemu bezpieczeństwa realizujący zadanie Firewall musi posiadać certyfikat ICSA lub EAL4+ lub równoważny dla rozwiązań kategorii Network Firewall. |
| Deklaracja zgodności UE (certyfikat CE) potwierdzająca spełnienie wymagań dyrektywy „Nowego Podejścia”. Urządzenie musi posiadać oznakowanie CE. |
| Certyfikat zgodności z dyrektywą RoHS lub dokument wystawiony przez niezależną, akredytowaną jednostkę potwierdzający spełnienie kryteriów środowiskowych zgodnych  z dyrektywą RoHS o eliminacji substancji niebezpiecznych. |

**Dostawa i montaż:**

Dostawa wraz z montażem w szafie krosowej u Zamawiającego oraz wstępną konfiguracją ustaloną z Zamawiającym.

Maksymalny czas realizacji tych działań został oszacowany w celu zachowania równego traktowania oferentów i wynosi 6 godzin zegarowych na miejscu u Zamawiającego. Jest to maksymalny czas przewidziany na wykonanie wskazanych czynności.

W przypadku napotkania problemów technicznych, wykonawca musi zapewnić dodatkowe wsparcie zadane w celu rozwiązania wszelkich potencjalnych komplikacji – czas nie jest wliczany do czasu „Rozszerzone wsparcie”.

**Rozszerzone wsparcie**

Do zamawianego produktu Wykonawca zapewni usługi wsparcia technicznego świadczone   
w języku polskim w zakresie co najmniej:

1. pomoc w prawidłowej i zgodnej z wymaganiami producenta rejestracji produktu;
2. zdalna rekonfiguracja produktu (połączenia szyfrowane) zgodnie z wymaganiami użytkownika max. 5 godzin zegarowych rozliczanych do 15 minut w terminie wsparcia produktu.

**CZĘŚĆ III – dostawa UPS dla stanowisk pracy**

Dostawa UPS dla stanowisk pracy w ilości – 69 sztuk w tym 40 szt. 600W i 29 szt. 500W

Zasilacze awaryjne UPS przy stanowiskach pracy poszczególnych użytkowników mają umożliwić ciągłość pracy w razie zaniku napięcia oraz w przypadku dłuższych przerw w dostawie prądu bezpiecznie zapisać dane, zapobiegając ich utracie.

UPS musi spełniać następujące minimalne wymagania:

* Moc stała: 600Wdla 40 szt. (500W dla 29 szt.)
* Moc pozorna: 1000VA dla 40 szt. (850VA dla 29 szt.)
* Napięcie: 220-230V (50/60Hz)
* Zakres napięcia: 162-285V
* Sprawność przy maks. obciążeniu: min 97%
* Częstotliwość: 50/60Hz+-1Hz
* Przebieg napięcia: Sinusoida modyfikowana
* Wyświetlacz LCD: tak
* Czas ładowania: maks. 12 godzin
* Czas podtrzymania: min. 2 minuty przy 100% obciążenia
* Czas przełączania maks. ms: 2-6ms
* Tryb podtrzymania (backup): Sygnał dźwiękowy
* Błąd: Ciągły sygnał
* Zabezpieczenia pełne: Przeciwzwarciowe; Przeciwprzepięciowe; Termiczne
* Dołączone oprogramowanie: tak w języku polskim
* Port komunikacyjny: USB
* Stabilizator napięcia sieciowego AVR
* Porty zasilania wy.: min. francuskie - 4 szt.;
* **Ogranicznik przepięć (ASR) spełniający wymagania normy IEC 616431-1.**
* Typ obudowy: Tower.
* Rodzaj: zasilacz typu line-interactive.
* Możliwość zimnego startu.
* Możliwość wymiany baterii przez użytkownika.
* Ochrona przed głębokim rozładowaniem.
* Deklaracja zgodności UE (Certyfikat CE). Urządzenie musi posiadać oznakowanie CE.
* Urządzenie musi być oznaczone etykietą WEEE.

**Dostawa i montaż:**

Dostawa do wskazanego pomieszczenia u Zamawiającego.

**CZĘŚĆ IV – Certyfikat SSL dla BIP Urzędu Gminy Milówka**

1. **Przedmiot zamówienia**

Zamówienie dotyczy dostawy, instalacji oraz konfiguracji certyfikatu SSL (Secure Sockets Layer) typu **OV SSL (Organization Validation)** dla strony internetowej BIP Urzędu Gminy Milówka (www.bip.milowka.com.pl), w celu zapewnienia bezpiecznej komunikacji z użytkownikami oraz ochrony danych przesyłanych pomiędzy użytkownikami a serwerem.

1. **Wymagania ogólne**

* Certyfikat SSL ma zapewniać pełne szyfrowanie danych przesyłanych pomiędzy użytkownikami a serwerem Urzędu Gminy Milówka.
* Certyfikat musi być wystawiony przez uznany urząd certyfikacji (CA - Certification Authority), zapewniający pełną zgodność z obowiązującymi standardami bezpieczeństwa.
* Certyfikat musi być zgodny z przepisami dotyczącymi ochrony danych osobowych (RODO) oraz z ustawą o krajowym systemie cyberbezpieczeństwa.
* Certyfikat SSL musi obsługiwać standardy szyfrowania TLS (Transport Layer Security) oraz zapewniać wysoką kompatybilność z popularnymi przeglądarkami internetowymi i systemami operacyjnymi.
* Certyfikat SSL musi być dostarczony z pełnym wsparciem w zakresie instalacji oraz konfiguracji.

1. **Typ certyfikatu SSL**

Zamawiający wymaga następującego typu certyfikatu SSL:

* **Certyfikattypu: OV SSL (Organization Validation)**
  + Certyfikat OV SSL zapewnia weryfikację tożsamości organizacji. Certyfikat OV SSL zapewnia odpowiedni poziom zaufania dla stron instytucji publicznych, takich jak Urząd Gminy Milówka.

1. **Ważność certyfikatu SSL**

Certyfikat SSL powinien być wystawiony na okres **24 miesięcy**.

1. **Wymagania dotyczące instalacji certyfikatu SSL**

* Instalacja certyfikatu na serwerze BIP Urzędu Gminy Milówka(BIP Urzędu Gminy Milówka znajduje się na zewnętrznym serwerze)powinna zostać przeprowadzona przez wykonawcę w sposób profesjonalny, zgodnie z najlepszymi praktykami w zakresie konfiguracji SSL.
* Po zainstalowaniu certyfikatu, wykonawca zobowiązany jest do przeprowadzenia testów weryfikujących poprawność jego działania, w tym testów szyfrowania oraz certyfikacji   
  na stronie bip.milowka.com.pl.
* Wykonawca musi również zapewnić przekierowanie z HTTP na HTTPS, aby wymusić bezpieczne połączenie na całej stronie internetowej.

1. **Wymagania dotyczące wsparcia technicznego**

* Wykonawca zobowiązuje się do zapewnienia wsparcia technicznego przez cały okres ważności certyfikatu SSL.
* Wsparcie techniczne powinno obejmować pomoc w przypadku problemów związanych   
  z instalacją, konfiguracją lub odnawianiem certyfikatu SSL.

1. **Gwarancja**  
   Wykonawca zapewnia gwarancję poprawnego działania certyfikatu SSL przez cały okres jego ważności. Gwarancja obejmuje:

* Wymianę certyfikatu w przypadku jego nieważności lub problemów z funkcjonowaniem.

1. **Wymagania dotyczące bezpieczeństwa**

* Certyfikat SSL musi zapewniać minimum 2048-bitowe klucze szyfrowania.
* Certyfikat musi być zgodny z aktualnymi standardami bezpieczeństwa i najnowszymi protokołami szyfrowania (TLS 1.2 lub TLS 1.3).
* Certyfikat musi być wystawiony przez zaufany urząd certyfikacji, który jest rozpoznawany przez wszystkie główne przeglądarki internetowe (np. Google Chrome, Mozilla Firefox, Microsoft Edge, Safari).

**CZĘŚĆ V ZAMÓWIENIA - Dostawa oprogramowania z zakresu systemu zarządzania bezpieczeństwem informacji i ochroną danych osobowych**

Dostawa oprogramowania z zakresu systemu zarządzania bezpieczeństwem informacji i ochroną danych osobowych, systemu zarządzania antykorupcją, kontroli zarządczej

I. Przedmiot zamówienia

Przedmiot zamówienia obejmuje zakup i dostawę 1 szt. specjalistycznego oprogramowania wspomagającego systemowe zarządzanie urzędem w zakresie bezpieczeństwa informacji   
i ochrony danych osobowych systemu zarządzania antykorupcją, kontroli zarządczej.

II. Typ dostarczonej licencji - Licencja produkcyjna programu.

Licencja na wszystkie bloki i moduły programu udzielana na czas nieokreślony, bez limitu użytkowników. Wsparcie producenta oprogramowania do 30 czerwca 2026. Dostawca   
do 30 czerwca 2026 zapewnia wsparcie, w ramach którego Zamawiający zostanie uprawniony do nieodpłatnego pobierania poprawek i aktualizacji oraz na bieżąco pomocy (nadzoru)   
w obsłudze programu.

III. Wymagania ogólne oprogramowania

1. Oprogramowanie ma być dostarczone w najnowszej wersji w języku polskim.

2. Oprogramowanie powinno posiadać dokumentację użytkownika opisującą funkcjonalność każdego z modułów oprogramowania oraz dokumentację administratora opisującą sposób administrowania programem w tym jego instalowania, konfiguracji, sposobu tworzenia kopii zapasowych oraz odtwarzania w przypadku awarii,

3. Program powinien umożliwiać pracę zarówno na komputerach stacjonarnych   
jak i na urządzeniach mobilnych np. smartfonach.

4. Program na komputerze klienckim powinien posiadać możliwość instalacji jako aplikacja PWA.

5. Koszt zakupu oprogramowania powinien uwzględniać koszt wszystkich składników oprogramowania (poza systemem operacyjnym zainstalowanym na serwerze Zamawiającego), które są niezbędne do jego pracy zgodnie z niniejszą specyfikacją.

6. W ramach zamówienia Zamawiający otrzyma wersję instalacyjną oprogramowania oraz licencję uprawniającą do korzystania z przedmiotowego oprogramowania.

IV. Techniczne dane oprogramowania

1. Program powinien pracować jako aplikacja intranetowa uruchamiana i prawidłowo pracująca w aktualnych wersjach przeglądarek internetowych (MS Edge, Google Chrome, FireFox).

2. Wszystkie dane gromadzone w oprogramowaniu powinny być zapisywane wyłącznie centralnie, na komputerze pełniącym rolę serwera pracującego w trybie ciągłym przez 24 godziny na dobę.

3. Serwer będzie dostarczony przez Zamawiającego i będzie znajdował się w jego siedzibie.

4. Program powinien pracować na serwerze z procesorem 8-rdzeniowy w architekturze 64 bit., min. 1TB SSD, min. 16GB RAM z zainstalowanym systemem Windows lub Linux (inne składniki oprogramowania niezbędne do pracy programu dostarcza Dostawca).

5. Aplikacja instalowana na serwerze działającym w systemie Windows powinna posiadać automatyczny instalator wszystkich składników niezbędnych do prawidłowego działania oprogramowania.

6. Poza instalatorem dla systemu Windows aplikacja powinna mieć możliwość uruchomienia na serwerze pracującym pod systemem Linux (konfiguracja instalacji niestandardowych powinna być określona w dokumentacji programu).

7. Program ma mieć możliwość importu użytkowników z przygotowanego zgodnie   
ze specyfikacją pliku lub ich importu bezpośrednio z Active Directory.

8. Program ma mieć możliwość opcjonalnej integracji z Active Directory.

V. Funkcjonalność oprogramowania i jego zakres działania

1. Specjalistyczne oprogramowanie do zarządzania urzędem w zakresie m.in. bezpieczeństwa informacji i ochrony danych osobowych musi posiadać funkcjonalności, które umożliwiają zarządzanie obszarami m.in.:

procesami realizowanymi w urzędzie – w tym zakresie oprogramowanie musi:

- posiadać rejestr zidentyfikowanych procesów w tym procesów z zakresu ochrony danych, który umożliwia ich podział na makroprocesy,

- posiadać możliwość opisu procesu poprzez określenie początku i końca procesu, danych wejściowych i wyjściowych procesu, dostawcę, klienta procesu, zakresu podmiotowego   
i przedmiotowego, dokumentów wymaganych w procesie oraz ryzyk wpływających na osiąganie celu procesów,

- posiadać graficzny edytor do tworzenia interaktywnych map procesów (z możliwością podpinania plików pod dowolne elementy grafu),komórkami organizacyjnymi – w tym zakresie oprogramowanie musi:

- posiadać rejestr komórek organizacyjnych, który będzie oparty na zatwierdzonym   
w Urzędzie regulaminie organizacyjnym,

- posiadać możliwość opisu komórki organizacyjnej poprzez określenie jej podrzędności   
w strukturze organizacyjnej, przypisania do niej stanowisk pracy oraz zakresu zadań jaki realizuje,stanowiskami pracy – w tym zakresie oprogramowanie musi:

- posiadać rejestr stanowisk pracy przypisanych do właściwych komórek organizacyjnych, zgodnie z obowiązującym regulaminem organizacyjnym,

- posiadać możliwość opisania stanowiska pracy poprzez określenie m.in.: miejsca stanowiska pracy w strukturze organizacyjnej, celu istnienia stanowiska pracy, liczby podległych pracowników, głównych zadań realizowanych na stanowisku pracy, wymaganych upoważnień i pełnomocnictw obowiązujących na danym stanowisku pracy oraz wymaganiach w zakresie kompetencji czy doświadczenia,pracownikami – w tym zakresie oprogramowanie musi:

- posiadać rejestr wszystkich pracowników, praktykantów i stażystów oraz osób świadczących pracę na umowach cywilnoprawnych,

- posiadać możliwość prześledzenia historii zatrudnienia pracownika, w zakresie   
m.in. obejmowanych stanowisk pracy, pełnionych przez niego funkcji i posiadanych uprawnień w aplikacjach przez niego eksploatowanych w organizacji,dokumentami – w tym zakresie oprogramowanie musi:

- posiadać rejestr wszystkich dokumentów określających wymagania (m.in.: polityk, zarządzeń, decyzji, instrukcji, procedur) obowiązujących na poszczególnych stanowiskach pracy w urzędzie,

- posiadać możliwość opisania dokumentu poprzez m.in.: określenie osoby odpowiedzialnej za dokument, przypisanie do procesu, który realizuje oraz wskazanie właściwych stanowisk pracy na jakich obowiązuje,

- posiadać możliwość udostępniania treści dokumentu pracownikom,

- posiadać możliwość elektronicznego wnioskowania o utworzenie bądź zmianę dokumentu, nadzorowania etapów jego tworzenia oraz opiniowania przez wytypowanych użytkowników przesłanego projektu dokumentu,

- posiadać możliwość dystrybucji zatwierdzonego dokumentu na stanowiska pracy, na których obowiązuje dokument,

- posiadać możliwość elektronicznego zapoznania się przez użytkownika, będącego jednocześnie pracownikiem urzędu, z dokumentem obowiązującym na zajmowanym przez niego stanowisku pracy i elektronicznego potwierdzenia zapoznania się z treścią dokumentu,

- posiadać narzędzia weryfikacji danych dotyczących potwierdzenia zapoznania pracowników z dokumentacją obowiązującą na ich stanowisku pracy,

założeniami wdrożonego w Urzędzie SZBI – w tym zakresie oprogramowanie musi:

- wspomagać opisywanie kontekstu organizacji w tym dokumentować okresowe analizy czynników mających wpływ na zdolność organizacji do osiągania zamierzonych celów, umożliwiać opisanie zakresu i wyłączeń systemu oraz potrzeb i oczekiwań stron zainteresowanych,

- udostępniać pracownikom przygotowaną w programie deklarację polityki bezpieczeństwa informacji wraz ze spójnymi z nią celami powiązanymi z procesami oraz wskaźnikami ich pomiarów,

- w sposób przejrzysty udostępniać pracownikom organizacji pełne wymagania systemu zarządzania bezpieczeństwem informacji i ochrony danych osobowych, w tym prezentować   
w formie graficznej wzajemne powiązania dokumentacji (tworzyć interaktywny schemat   
z możliwością otwierania poszczególnych dokumentów po kliknięciu na elementy grafu).

sprzętem komputerowym i oprogramowaniem komputerowym – w tym zakresie oprogramowanie musi:

- posiadać rejestr wszystkich urządzeń informatycznych oraz zainstalowanego na nim oprogramowania komputerowego,

- mieć możliwość automatycznego sczytywania parametrów sprzętowych i oprogramowania zainstalowanego na komputerach działających pod kontrolą systemu operacyjnego Windows,  
- posiadać możliwość ewidencjonowania bieżących przeglądów sprzętu komputerowego oraz zainstalowanego na nim oprogramowania,

- posiadać możliwość elektronicznego zgłaszania usterek i awarii sprzętu komputerowego,  
- posiadać możliwość ewidencjonowania rodzaju umów serwisowych na sprzęt komputerowy,

- posiadać możliwość ewidencjonowania i zarządzania materiałami eksploatacyjnymi niezbędnymi do pracy sprzętów komputerowych np. tonery do drukarek,

- posiadać możliwość ewidencji wszystkich zdarzeń, czynności naprawczych, serwisowych czy konserwacyjnych komputerów lub serwera.

licencjami na oprogramowanie – w tym zakresie oprogramowanie musi:

- posiadać rejestr licencji oprogramowania komputerowego zainstalowanego na komputerach w Urzędzie oraz rejestr umów licencyjnych podpisanych przez Urząd na dostawę specjalistycznego oprogramowania,

- posiadać możliwość ewidencji posiadanych przez Urząd umów na korzystanie z licencji programów komputerowych,

obsługą problemów zgłaszanych przez użytkowników – w tym zakresie oprogramowanie musi:

- dostarczać użytkownikom kanał komunikacji do zgłaszania problemów z obszaru IT,

- dokumentować obsługę zgłoszeń oraz nadzorować terminowości ich realizacji,

- określać kategorie zgłoszeń i ustalać osoby odpowiedzialne za ich obsługę,

aktywami informacyjnymi – w tym zakresie oprogramowanie musi:

- umożliwiać prowadzenie rejestru zidentyfikowanych aktywów informacyjnych oraz zasobów wspomagających,

- wspomagać opisywanie aktywów m.in. poprzez wskazanie procesów przetwarzających informacje oraz istotności informacji dla realizacji danego procesu, wskazanie zasobów wykorzystywanych przy przetwarzaniu informacji oraz określenie poziomu istotności zasobu dla informacji,

- umożliwiać ustalenie wymaganego poziomu podstawowych oraz dodatkowych atrybutów informacji i adekwatnie do tego ustalać klasyfikacje aktywów.

ochrony danych osobowych – w tym zakresie oprogramowanie musi:

- umożliwiać prowadzenie zgodnie z przepisami prawa rejestru czynności przetwarzania i kategorii czynności przetwarzania danych osobowych w Urzędzie,

- posiadać możliwość rejestrowania klauzul informacyjnych udostępnianych przez Urząd, a w przypadku klauzul kierowanych do pracowników program automatycznie informuje pracowników o konieczności zapoznania się z klauzulą informacyjną i udostępnia użytkownikom uprawnionym informacje o dacie zapoznania się pracowników z poszczególnymi klauzulami informacyjnymi,

- posiadać możliwość ewidencji zawartych przez Urząd umów powierzenia przetwarzania danych osobowych,

- wspomagać wystawianie upoważnień do przetwarzania danych osobowych oraz prowadzić rejestr osób upoważnionych do przetwarzania danych osobowych,

- posiadać elektroniczny rejestr udostępnionych danych osobowych, który zawiera   
m.in. informacje o wnioskującym, dacie wniosku, podstawie prawnej upoważniającej   
do udostępnienia danych, zakresie udostępnionej informacji oraz terminie i osobie udostępniającej,

- umożliwiać ewidencjonowanie oraz wspomagać obsługę wniosków wynikających z RODO tj.:

- dostęp do danych osobowych (art. 15 RODO),

- sprostowanie danych osobowych (art. 16 RODO),

- usunięcie danych osobowych (art. 17 RODO),

- ograniczenie przetwarzania danych osobowych (art. 18 RODO),

- przeniesienie danych osobowych (art. 20 RODO),

- sprzeciw wobec przetwarzania danych osobowych (art. 21 RODO),

zarządzaniem ryzykiem bezpieczeństwa informacji – w tym zakresie oprogramowanie musi:

- posiadać rejestr zidentyfikowanych ryzyk w zakresie m.in. bezpieczeństwa informacji   
i ochrony danych osobowych,

- posiadać możliwość przypisania stanowiska odpowiedzialnego za zidentyfikowane ryzyko   
i jego cyklicznej oceny,

- posiadać możliwość identyfikacji i ewidencji czynników ryzyka (źródeł zagrożeń i szans), podatności na zagrożenia lub szanse, opisania skutków ryzyka, estymację i ocenę ryzyka, ustalenia reakcji na ryzyko oraz monitorowania i raportowania ryzyka,

- posiadać możliwość przeprowadzania cyklicznej oceny ryzyka,

- prezentować ryzyka w formie graficznych zestawień m.in. mapy ryzyka,

zarządzania uprawnieniami użytkowników w aplikacjach – w tym zakresie oprogramowanie musi:

- posiadać rejestr wszystkich aplikacji użytkowanych w Urzędzie,

- posiadać rejestr nadanych w Urzędzie uprawnień do przetwarzania danych w aplikacjach komputerowych zgodnie z zakresem zadań wykonywanych przez pracownika,

- posiadać możliwość elektronicznego wnioskowania o nadanie właściwych uprawnień   
dla pracowników zgodnie z ich zakresem obowiązków do obsługi programów komputerowych, w których są przetwarzane dane osobowe,

- w przypadku aplikacji przetwarzających dane osobowe weryfikować czy pracownik posiada upoważnienie do przetwarzania danych osobowych,

- ustalać etapy przetwarzania wniosku m.in. akceptację, opiniowanie zatwierdzanie,

- informować użytkowników odpowiedzialnych za realizację danego etapu przetwarzania wniosku o konieczności jego zrealizowania,

- posiadać możliwość elektronicznego potwierdzenia przez pracownika zapoznania   
się z zakresem nadanego uprawnienia,incydentami i słabościami systemu – w tym zakresie oprogramowanie musi:

- posiadać rejestr zaistniałych incydentów oraz słabości systemu,

- posiadać możliwość zgłoszenia zidentyfikowanego zdarzenia lub słabości systemu bezpieczeństwa informacji (w tym naruszenia ochrony danych osobowych),

- umożliwiać analizę i klasyfikację zgłoszonego zdarzenia,

- wspomagać obsługę incydentów bezpieczeństwa informacji w tym określenia operatora incydentu oraz ewidencjonować podejmowane działania,

- posiadać stosowne zestawienia dotyczące zidentyfikowanych incydentów i słabości systemów w Urzędzie,certyfikatami bezpieczeństwa – w tym zakresie oprogramowanie musi:

- posiadać rejestr certyfikatów bezpieczeństwa,

- posiadać możliwość wnioskowania o nadanie certyfikatu bezpieczeństwa,

- umożliwiać użytkownikom uprawnionym ewidencjonowanie certyfikatów bezpieczeństwa,

- umożliwiać elektroniczne potwierdzenia posiadania przez pracownika certyfikatu bezpieczeństwa,

- informować użytkowników uprawnionych o zbliżającym się terminie ważności certyfikatu   
i nadzorować etapy jego odnowienia,

- posiadać możliwość unieważniania certyfikatu bezpieczeństwa,wewnętrznymi audytami   
w zakresie bezpieczeństwa informacji i ochroną danych osobowych – w tym zakresie oprogramowanie musi:

- posiadać rejestr przeprowadzonych w Urzędzie audytów wewnętrznych w tym auditów  
w zakresie bezpieczeństwa informacji i ochrony danych osobowych,

- posiadać możliwość tworzenia programów auditów wewnętrznych na dany rok   
oraz planowania auditów z określeniem m.in.: zakresu auditu, przedmiotu auditu, komórek organizacyjnych uczestniczących w działaniach auditowych, terminu przeprowadzenia audytu oraz osób przeprowadzających audit,

- możliwość dokumentowania podjętych działań auditowych tj. przygotowanie m.in.: programu audytów na dany rok, protokołu końcowego z audytu,

- możliwość dokumentowania wszystkich spostrzeżeń, niezgodności i wniosków wynikłych podczas podjętych działańaudytowych.,

- możliwość zgłoszenia zauważonych podczas auditu niezgodności do właściwej osoby odpowiedzialnej,

działaniami doskonalącymi – w tym zakresie oprogramowanie musi:

- posiadać rejestr wszystkich zidentyfikowanych w Urzędzie nieprawidłowości (niezgodności) w zakresie bezpieczeństwa informacji i ochrony danych osobowych,

- posiadać możliwość elektronicznego zgłaszania zidentyfikowanych nieprawidłowości   
w funkcjonowaniu systemu bezpieczeństwa informacji i ochrony danych osobowych,

- możliwość analizy zgłoszonej nieprawidłowości przez osoby za to odpowiedzialne,

- możliwość określenia działań korygujących i korekcyjnych względem zidentyfikowanej nieprawidłowości oraz zgłoszenia wykonania działań korygujących,przeglądami zarządzania   
w zakresie bezpieczeństwa informacji i ochroną danych osobowych – w tym zakresie oprogramowanie musi:

- posiadać rejestr przeprowadzanych w Urzędzie cyklicznych przeglądów zarządzania   
w zakresie m.in. bezpieczeństwa informacji i ochrony danych osobowych,

- możliwość automatycznego przygotowania raportu do analizy z zakresu   
m.in. bezpieczeństwa informacji i ochrony danych osobowych.

2. Wszystkie moduły programu muszą być ze sobą kompatybilne i wzajemnie powiązane (moduły powinny korzystać z danych wprowadzanych w innych modułach bez konieczności ponownego ewidencjonowania tych samych danych).

3. Program musi informować użytkownika o działaniach, które musi podjąć w aplikacji   
ze względu na posiadane w aplikacji uprawnienia lub zajmowane w organizacji stanowisko pracy.

4. Komunikaty adresowane do użytkowników muszą być dostępne po zalogowaniu użytkownika do bezpośrednio aplikacji i w formie powiadomień PUSH oraz równolegle wysyłane na adres e-mail użytkownika.

5. Z poziomu komunikatu przesłanego pocztą elektroniczną użytkownik może przejść bezpośrednio do modułu w programie, w którym musi podjąć działania.

VI. Licencja

1. Licencja ma być przyznana na czas nieograniczony.

2. Licencja ma zezwalać na jednoczesną pracę w programie wszystkich pracowników Urzędu.

3. Licencja nie może ograniczać liczby końcówek jednocześnie korzystających   
z oprogramowania.

4. Licencja musi dopuszczać tworzenie przez Zamawiającego dowolnej ilości kopii oprogramowania dla celów testowych lub szkoleniowych.

**Instalacja i konfiguracja oprogramowania**

* **Instalacja oprogramowania**: Zainstalowanie oprogramowania na serwerach oraz komputerach roboczych w Urzędzie Gminy Milówka.
* **Konfiguracja systemu**: Dostosowanie ustawień oprogramowania do potrzeb użytkowników i procesów w Urzędzie. Konfiguracja takich funkcji jak:
  + Zarządzanie dokumentami.
  + Automatyzacja obiegu dokumentów.
* **Konfiguracja dostępu**: Ustalenie ról użytkowników i uprawnień, zapewnienie odpowiednich poziomów dostępu do dokumentów i procesów w systemie.
* **Ustalenie procedur bezpieczeństwa**: Zdefiniowanie zasad ochrony danych osobowych oraz zabezpieczeń systemowych zgodnie z RODO i normami bezpieczeństwa.

**CZĘŚĆ VI ZAMÓWIENIA**: **Dostawa agregatu prądotwórczego generatora – z przyłączem do zasilania awaryjnego budynku**

1. **Zasilanie awaryjne budynku Urzędu Gminy Milówka**

**Termin realizacji zamówienia – do 120 dni od dnia podpisania umowy.**

* 1. **Dostawa agregatu prądotwórczego - generatora – z przyłączem do zasilania awaryjnego budynku Urzędu Gminy Milówka**

Zamawiający posiada trójfazowe przyłącze energetyczne, o mocy umownej 30 kW, wraz z mikroinstalacją fotowoltaiczną o mocy 12,18 kWp.

1. Przedmiot zamówienia obejmuje:

* ~~zaprojektowanie podłączenia, wraz z układem SZR (Samoczynnego Załączania Rezerwy), wykonanie Instrukcji Eksploatacyjno- Ruchowej Agregatu, Instrukcji Współpracy Ruchowej oraz niezbędne uzgodnienia Tauron Dystrybucja S.A. (jeśli dotyczy~~),
* ~~uzgodnienie z rzeczoznawcą p.poż lokalizacji agregatu, jego przyłączenia (jeśli dotyczy),~~
* dostawę agregatu prądotwórczego do zasilania awaryjnego wraz z przyłączem - SZR do budynku Urzędu,
* ~~fundamentowanie i posadowienie agregatu,~~
* ~~wykonanie uziemienia agregatu i połączenie go z uziemieniem budynku Urzędu Gminy,~~
* ~~wykonanie zabezpieczenia ogrodzenia agregatu uniemożliwiające dostęp osób postronnych.~~
* podłączenie do instalacji,
* pierwsze uruchomienie wraz z zatankowaniem do pełna agregatu,
* szkolenie pracowników.

1. Oferowany sprzęt musi być :

* fabrycznie nowy
* rok produkcji min. 2025 r.
* nieużywany
* sprawny technicznie
* bez wad i uszkodzeń mechanicznych
* zmontowany i gotowy do użytku
* wolny od wad fizycznych i prawnych
* spełniać wymagania techniczno-użytkowe zamawiającego i obowiązujące prawem standardy jakościowe i normatywne obowiązujące na dzień realizacji zamówienia.

1. Agregat musi posiadać następujące wymagania i parametry:

* Agregat stacjonarny w obudowie przystosowanej do eksploatacji na zewnątrz, odporny na czynniki atmosferyczne typowe dla polskiej strefy klimatycznej, wyposażony w układ wspomagający rozruch w niskich temperaturach.
* Agregat producenta europejskiego z serwisem dostępnym w Polsce,
* Moc nominalna 3f. min. 56kVA/45kW (zgodnie z ISO8528)
* Napięcie 400V/230V,
* Częstotliwość 50 Hz,
* Rodzaj paliwa: olej napędowy
* Zużycie paliwa: do 17 l/h
* Zbiornik na paliwo: min. 120l.
* Prądnica synchroniczna, samowzbudna, bezszczotkową, posiadająca automatyczny, elektroniczny regulator napięcia prądnicy, zapewniający stabilność napięcia ± 1,0 % w całym zakresie obciążenia, - współczynnik zawartości harmonicznych THD (bez obciążenia) < 3,0 %.
* Wersja stacjonarna w obudowie/wyciszony, przystosowany do pracy na zewnątrz.
* Agregat musi mieć możliwość rozruchu manualnego i automatycznego,
* Automatyka przystosowana do pracy z mikroinstalacją fotowoltaiczną,
* Agregat powinien być wyposażony w akumulator, płyny eksploatacyjne, paliwo w ilości niezbędnej do przeprowadzenia prób i startu, wyłącznik awaryjny STOP na obudowie,
* Panel sterowania z interfejsem graficznym w języku polskim.

1. Wymagania zamawiającego do kompletacji agregatu:
   1. silnik

* producent europejski z serwisem dostępnym w Polsce
* rzędowy diesel
* moc min.45kW
* zużycie paliwa max.17 l/h
* instalacja elektryczna autonomiczna 12V lub 24V
* elektroniczna regulacja obrotów
* układ zasilania - bezpośredni wtrysk
* czas pracy na pełnym zbiorniku przy 100% obciążenia min. 7h
* tłumik z kompensatorem drgań
  1. prądnica:
* samowzbudna, synchroniczna, bezszczotkowa,
* trzyfazowa,
* uzwojenia odporne na wilgoć,
* regulacja napięcia AVR elektroniczna,
* stabilność napięcia do ±1%,
* stopień ochrony IP23.
  1. obudowa:
* stal zabezpieczona antykorozyjnie, pomalowana proszkowo,
* odporna na działania atmosferyczne,
* mocowanie na wibroizolatorach,
* izolacja akustyczna (wyciszenie).

1. Wymagania Zamawiającego dotyczące przyłącza.

* Aparaturę łączeniową zamontować w skrzynce przystosowanej do montażu zewnętrznego, odpornej na działanie czynników atmosferycznych,
* Automatyka SZR dostarczona razem z agregatem powinna automatycznie przełączać  
  i uruchamiać agregat w przypadku braku napięcia sieciowego.
* Skrzynię z automatyką SZR zainstalować przy ścianie budynku Urzędu Gminy,