

ZAMAWIAJĄCY:

Gmina Góra Świętej Małgorzaty,
Góra Świętej Małgorzaty 44, 99-122 Góra Świętej Małgorzaty
NIP: 7752405513

OPIS PRZEDMIOTU ZAMÓWIENIA

Na potrzeby postępowania o udzielenie zamówienia publicznego pn.: „**Dostawa oprogramowania dla Urzędu Gminy zwiększająca odporność na cyberataki wraz z wdrożeniem w ramach realizacji grantu pn. : Cyberbezpieczny Samorząd**” w ramach Projektu Cyberbezpieczny Samorząd realizowanego w ramach Funduszy Europejskich na Rozwój Cyfrowy 2021-2027 (FERC) Priorytet II: Zaawansowane usługi cyfrowe, Działanie 2.2. – Wzmocnienie krajowego systemu cyberbezpieczeństwa, **w zakresie dostawy oprogramowania wspierającego system zarządzania bezpieczeństwem informacji.**

Wymagania ogólne

W przypadkach, kiedy w szczegółowym opisie przedmiotu zamówienia wskazane zostały znaki towarowe, patenty, pochodzenie, źródło lub szczególny proces, który charakteryzuje produkty lub usługi dostarczane przez konkretnego Wykonawcę, co prowadziłoby do uprzywilejowania lub wyeliminowania niektórych wykonawców lub produktów, oznacza to, że Zamawiający nie może opisać przedmiotu zamówienia za pomocą dostatecznie dokładnych określeń i jest to uzasadnione specyfiką przedmiotu zamówienia. W takich sytuacjach ewentualne wskazania na znaki towarowe, patenty, pochodzenie, źródło lub szczególny proces, należy odczytywać z wyrazami „lub równoważne”. Dostarczany sprzęt musi być fabrycznie nowy, nieużywany, nieregenerowany, kompletny, wyprodukowany nie wcześniej niż w 2024 r., wolny od jakichkolwiek wad fizycznych i prawnych, sprawny technicznie, pochodzić z oficjalnego kanału dystrybucyjnego. Przez stwierdzenie "fabrycznie nowy" należy rozumieć sprzęt opakowany oryginalnie (opakowanie musi być nienaruszone i posiadać zabezpieczenie zastosowane przez producenta). Przez "wadę fizyczną" należy rozumieć również jakąkolwiek niezgodność ze szczegółowym opisem przedmiotu zamówienia. Sprzęt musi być wyposażony we wszystkie niezbędne do jego działania i zapewnienia wymaganych funkcjonalności Sprzętu standardowe rozwiązania softwarowe wraz z prawem do bezterminowego korzystania przez Zamawiającego z tych rozwiązań w takiej funkcji, jednakże w każdym przypadku nie krócej, niż przez czas, w jakim będzie technicznie możliwe używanie Sprzętu. O ile inaczej nie zaznaczono, wszelkie zapisy SOPZ zawierające parametry techniczne należy odczytywać jako parametry minimalne.

1. Oprogramowanie wspierające system zarządzania bezpieczeństwem informacji

Przedmiot zamówienia	Minimalne wymagania Zamawiającego
1. Oprogramowanie wspierające system zarządzania bezpieczeństwem informacji	<ol style="list-style-type: none"> Oprogramowanie wspomagające zarządzanie w zakresie bezpieczeństwa informacji i ochrony danych osobowych. Oprogramowanie ma być dostarczone w najnowszej wersji w języku polskim. Oprogramowanie powinno posiadać dokumentację użytkownika opisującą funkcjonalność każdego z modułów oprogramowania. Wykonawca zainstaluje program na zasobach Zamawiającego. 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. W ramach zamówienia Zamawiający otrzyma licencję uprawniającą do korzystania z przedmiotowego oprogramowania. Program powinien pracować jako aplikacja intranetowa uruchamiana i prawidłowo pracująca w aktualnych wersjach przeglądarek internetowych (MS Edge, Google Chrome, FireFox). Wszystkie dane gromadzone w oprogramowaniu powinny być zapisywane wyłącznie centralnie, na komputerze pełniącym rolę serwera pracującego w trybie ciągłym przez 24 godziny na dobę. Serwer będzie dostarczony przez Zamawiającego i będzie znajdował się w jego siedzibie. Program powinien pracować na serwerze z procesorem 8-rdzeniowy w architekturze 64 bit, min. 256 SSD, min. 16GB RAM z zainstalowanym systemem operacyjny Windows lub Linux (inne składniki oprogramowania niezbędne do pracy programu dostarcza Wykonawca). Oprogramowanie musi: <ul style="list-style-type: none"> - posiadać rejestr zidentyfikowanych procesów w tym procesów z zakresu ochrony danych, - posiadać rejestr komórek organizacyjnych, który będzie oparty na regulaminie organizacyjnym, - posiadać możliwość opisu komórki organizacyjnej poprzez określenie jej podrzędności w strukturze organizacyjnej, przypisania do niej pracowników - posiadać rejestr wszystkich pracowników, praktykantów i stażystów oraz osób świadczących pracę na umowach cywilnoprawnych, - umożliwiać prowadzenie rejestru zidentyfikowanych aktywów informacyjnych oraz zasobów wspomagających, - umożliwiać prowadzenie zgodnie z przepisami prawa rejestru czynności przetwarzania i kategorii czynności przetwarzania danych osobowych w Urzędzie,

- posiadać możliwość rejestrowania klauzul informacyjnych
 - posiadać możliwość ewidencji zawartych umów powierzenia przetwarzania danych osobowych,
 - wspomagać wystawianie upoważnień do przetwarzania danych osobowych oraz prowadzić rejestr osób upoważnionych do przetwarzania danych osobowych,
 - posiadać możliwość identyfikacji i ewidencji czynników ryzyka (źródeł zagrożeń), podatności na zagrożenia lub szanse, opisanie skutków ryzyka, estymację i ocenę ryzyka,
 - posiadać możliwość przeprowadzania cyklicznej oceny ryzyka,
 - prezentować ryzyka w formie graficznych zestawień m.in. mapy ryzyka,
 - posiadać rejestr wszystkich użytkowanych aplikacji,
 - 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,
 - posiadać rejestr zaistniałych incydentów oraz słabości systemu,
 - posiadać rejestr przeprowadzonych audytów wewnętrznych w tym audytów w zakresie bezpieczeństwa informacji i ochrony danych osobowych,
 - posiadać moduł przeznaczony do kompleksowego prowadzenia oceny skutków dla ochrony danych osobowych, obejmującej identyfikację procesów przetwarzania, analizę ryzyka, ocenę zgodności z wymaganiami RODO oraz dokumentowanie zastosowanych środków minimalizujących ryzyko.
- System umożliwi uporządkowane gromadzenie informacji, prowadzenie analizy w ujednoliconym formularzu, zapisywanie wyników oraz generowanie dokumentacji niezbędnej do wykazania rozliczalności administratora danych.
- posiadać możliwość tworzenia programów audytów wewnętrznych na danych rok oraz planowania audytów z określeniem m.in.: zakresu audytu, przedmiotu audytu, komórek organizacyjnych uczestniczących w działaniach audytowych, terminu przeprowadzenia audytu oraz osób przeprowadzających audyt,
 - posiadać rejestr wszystkich zidentyfikowanych nieprawidłowości (niezgodności) w zakresie bezpieczeństwa informacji i ochrony danych osobowych,
11. 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).
12. Program musi informować o działaniach, które należy podjąć ze względu na posiadane w aplikacji uprawnienia lub zajmowane w organizacji stanowisko pracy.
13. Licencja:
- 1) Licencja ma zezwalać na jednoczesną pracę w programie wszystkich pracowników Urzędu.
 - 2) Licencja nie może ograniczać liczby końcówek jednocześnie korzystających z oprogramowania.
 - 3) Licencja musi dopuszczać tworzenie przez Zamawiającego dowolnej ilości kopii oprogramowania dla celów testowych lub szkoleniowych.

- | | |
|--|--|
| | <p>4) Od dnia przekazania przez 24 miesiące Wykonawca zapewnia wsparcie, w ramach którego Zamawiający zostanie uprawniony do nieodpłatnego pobierania poprawek i aktualizacji oraz na bieżąco pomocy (nadzoru) w obsłudze programu.</p> <p>5) Pomoc techniczna powinna być świadczona co najmniej w dni robocze w godzinach pracy Urzędu</p> |
|--|--|

