



Fundusze Europejskie  
na Rozwój Cyfrowy



Rzeczpospolita  
Polska

Dofinansowane przez  
Unię Europejską



CENTRUM  
PROJEKTÓW  
POLSKA  
CYFROWA

**GMINA SKOŁYSZYN**

GPIB.271.2.50.2025.12

tel./fax 13 44 910 62 (53) (64)

NIP 685-16-51-203 REGON 370440382

BS O/ Skołyszyn

76 8627 1037 2003 5000 0459 0001

## OPIS PRZEDMIOTU ZAMÓWIENIA

### Szkolenia specjalistyczne dla informatyków

Załącznik nr 1 do Zapytania Ofertowego

## 1 ZAMAWIAJĄCY

Gmina Skołyszyn, Skołyszyn 12, 38-242 Skołyszyn, NIP: 685-16-51-203, REGON: 370440382, email: [gmina@skolyszyn.pl](mailto:gmina@skolyszyn.pl)

## 2 OPIS PRZEDMIOTU ZAMÓWIENIA

Część zamówienia	Nazwa szkolenia	Liczba uczestników szkolenia
1.	FortiGate Administrator	1
2.	Wdrażanie, zarządzanie i zabezpieczanie sieci za pomocą zasad grupy	1
3.	Veeam® Backup & Replication™: Configure, Manage, and Recover (VMCE)	1

### 2.1 CZĘŚĆ 1 FORTIGATE ADMINISTRATOR

Forma szkolenia	Szkolenie online
Czas trwania szkolenia	32 godz. dydaktycznych (4 dni)
Język szkolenia	Polski <i>Jeżeli trener nie posługuje się językiem polskim Wykonawca zobowiązany jest zapewnić tłumaczenie</i>
Okres realizacji	do 120 dni po podpisaniu umowy
Przełanki dla szkolenia	Z uwagi na fakt, iż Zamawiający użytkuje rozwiązania Fortinet konieczne jest podniesienie kompetencji personelu informatycznego w zakresie administracji tymi rozwiązaniami.  Zamawiający wymaga przeprowadzenia szkolenia certyfikowanego przez firmę Fortinet w zakresie wymaganym przez producenta oprogramowania dostępnym na stronie



	<a href="https://training.fortinet.com/">https://training.fortinet.com/</a>
Program szkolenia / podstawowe kwestie poruszone na szkoleniu	<p>Program szkolenia:</p> <ul style="list-style-type: none"> <li>• System and Network Settings</li> <li>• Firewall Policies and NAT</li> <li>• Routing</li> <li>• Firewall Authentication</li> <li>• Fortinet Single Sign-On (FSSO)</li> <li>• Certificate Operations</li> <li>• Antivirus</li> <li>• Web Filtering</li> <li>• Intrusion Prevention and Application Control</li> <li>• SSL VPN</li> <li>• IPsec VPN</li> <li>• SD-WAN Configuration and Monitoring</li> <li>• Security Fabric</li> <li>• High Availability</li> <li>• Diagnostics and Troubleshooting</li> </ul>
Egzamin	Niewymagany
Wymagania wobec wykładowcy / trenera	<ul style="list-style-type: none"> <li>• Minimum 2-letnie doświadczenie z zakresu realizacji szkoleń dotyczących cyberbezpieczeństwa oraz rozwiązań UTM. Wymóg 2-letniego doświadczenia należy rozumieć jako przeprowadzenie co najmniej 4 szkoleń z tematyki objętej zakresem przedmiotu zamówienia w ciągu ostatnich 3 lat licząc wstecz od dnia opublikowania niniejszego zapytania. Przy czym szkolenia były realizowane w ciągu 2 różnych lat kalendarzowych. Doświadczenie należy wykazać w wykazie osób.</li> <li>• Aktualny certyfikat potwierdzający wiedzę z zakresu szkolenia wydany przez producenta sprzętu lub niezależną instytucję certyfikującą. Zamawiający będzie akceptował certyfikaty wydane przez producenta danego rozwiązania i powszechnie uznane certyfikaty informatyczne z obszaru szkolenia.</li> </ul> <p><b>Kopię certyfikatu należy dołączyć do oferty.</b></p>

## 2.2 CZĘŚĆ 2: WDRAŻANIE, ZARZĄDZANIE I ZABEZPIECZANIE SIECI ZA POMOCĄ ZASAD GRUPY

Forma szkolenia	Szkolenie online
Czas trwania szkolenia	40 godz. dydaktycznych (5 dni)
Język szkolenia	<p>Polski</p> <p><i>Jeżeli trener nie posługuje się językiem polskim Wykonawca zobowiązany jest zapewnić tłumaczenie</i></p>

Okres realizacji	do 120 dni po podpisaniu umowy,
Przestanki dla szkolenia	<p>Z uwagi na fakt, iż Zamawiający użytkuje rozwiązania Windows Serwer konieczne jest podniesienie kompetencji personelu informatycznego w zakresie administracji tymi rozwiązaniami.</p> <p>Zamawiający wymaga przeprowadzenia szkolenia certyfikowanego przez firmę Microsoft.</p>
Program szkolenia / podstawowe kwestie poruszone na szkoleniu	<p>Program szkolenia powinien być zgodny z programem szkolenia firmy Microsoft nr MS 50255 i obejmować co najmniej następujące zagadnienia:</p> <ul style="list-style-type: none"> <li>• Wprowadzenie do Group Policy</li> <li>• Narzędzia zarządzania Group Policy</li> <li>• Projektowanie infrastruktury Group Policy</li> <li>• Rozwiązywanie problemów z Group Policy</li> <li>• Wdrażanie szablonów zabezpieczeń</li> <li>• Wdrażanie zabezpieczeń za pomocą Group Policy</li> <li>• Konfiguracja środowiska stacji roboczych</li> <li>• Przypisywanie i publikowanie pakietów aplikacji</li> <li>• Systems Management Server</li> <li>• Tworzenie i wdrażanie szablonów administracyjnych (ADM)</li> <li>• Nowe funkcje Group Policy w Windows 8.1 i Windows Server 2012 R2</li> <li>• Zarządzanie preferencjami Group Policy</li> </ul>
Egzamin	niewymagany
Wymagania wobec wykładowcy / trenera	<ul style="list-style-type: none"> <li>• Minimum 2-letnie doświadczenie z zakresu realizacji szkoleń dotyczących rozwiązań z zakresu systemu Windows Serwer i jego bezpieczeństwa. Wymóg 2-letniego doświadczenia należy rozumieć jako przeprowadzeniu co najmniej 4 szkoleń z tematyki objętej projektem w ciągu ostatnich 3 lat licząc wstecz od dnia opublikowania niniejszego zapytania. Przy czym szkolenia były realizowane w ciągu 2 różnych lat kalendarzowych. Doświadczenie należy wykazać w wykazie osób.</li> <li>• Aktualny certyfikat potwierdzający wiedzę z zakresu szkolenia wydany przez producenta sprzętu lub niezależną instytucję certyfikującą. Zamawiający będzie akceptował certyfikaty wydane przez producenta danego rozwiązania i powszechnie uznane certyfikaty informatyczne z obszaru szkolenia. <b>Kopię certyfikatu należy dołączyć do oferty.</b></li> </ul>

### 2.3 CZĘŚĆ 3: VEEAM® BACKUP & REPLICATION™: CONFIGURE, MANAGE, AND RECOVER (VMCE)



Forma szkolenia	Szkolenie online
Czas trwania szkolenia	32 godz. dydaktycznych (4 dni)
Język szkolenia	Polski <i>Jeżeli trener nie posługuje się językiem polskim Wykonawca zobowiązany jest zapewnić tłumaczenie</i>
Okres realizacji	do 120 dni po podpisaniu umowy,
Przestanki dla szkolenia	Z uwagi na fakt, iż w ramach projektu Cyberbezpieczny Samorząd Zamawiający zakupił i użytkuje rozwiązania firmy Veem konieczne jest podniesienie kompetencji personelu informatycznego w zakresie administracji tymi rozwiązaniami.  Zamawiający wymaga przeprowadzenia szkolenia przez jednostkę szkoleniową certyfikowaną przez producenta oprogramowania lub przez oficjalnego partnera technologicznego producenta oprogramowania.
Program szkolenia / podstawowe kwestie poruszone na szkoleniu	Program Szkolenia: <ul style="list-style-type: none"> <li>• Strategie ochrony danych</li> <li>• Scenariusze ryzyka</li> <li>• Podstawowe komponenty</li> <li>• Przegląd komponentów Veeam Backup &amp; Replication</li> <li>• Początkowe rozważania dotyczące bezpieczeństwa</li> <li>• Tworzenie kopii zapasowych maszyn wirtualnych</li> <li>• Tworzenie kopii zapasowych za pomocą agenta</li> <li>• Tworzenie kopii zapasowych nieustrukturyzowanych danych</li> <li>• Optymalizacja przechowywania kopii zapasowych</li> <li>• Niezmiennność i utwardzone repozytoria</li> <li>• Przechowywanie obiektowe</li> <li>• Tryby transportu</li> <li>• Kopie backupu</li> <li>• Rozproszone Repozytorium Backup (Scale-out Backup Repository™)</li> <li>• Przenoszenie lub kopiowanie backupów</li> <li>• Replikacja</li> <li>• Weryfikacja możliwości odzyskania</li> <li>• Veeam Backup Enterprise Manager</li> <li>• Planowanie reagowania na incydenty</li> <li>• Scenariusze odnowienia systemu a cechy odnowienia</li> <li>• Uruchomienie procedury odnowienia systemu</li> <li>• Platforma Danych Veeam</li> </ul>
Egzamin	niewymagany
Wymagania wobec wykładowcy / trenera	<ul style="list-style-type: none"> <li>• Minimum 2-letnie doświadczenie z zakresu realizacji szkoleń dotyczących rozwiązań z zakresu systemów backupu firmy VEEM.</li> </ul> <p>Wymóg 2-letniego doświadczenia należy rozumieć jako przeprowadzeniu co najmniej 4 szkoleń z tematyki objętej projektu w ciągu ostatnich 3 lat licząc wstecz od dnia opublikowania niniejszego zapytania.</p>



	<p>Doświadczenie należy wykazać w wykazie osób.</p> <ul style="list-style-type: none"> <li>• Autoryzacja trenerska firmy VEEM.</li> <li>• Aktualny certyfikat potwierdzający wiedzę z zakresu szkolenia wydany przez producenta sprzętu lub niezależną instytucję certyfikującą. Zamawiający będzie akceptował certyfikaty wydane przez producenta danego rozwiązania i powszechnie uznane certyfikaty informatyczne z obszaru szkolenia.</li> </ul> <p>Kopię certyfikatu należy dołączyć do oferty.</p>
--	--

### 3 SZCZEGÓŁOWE INFORMACJE DOTYCZĄCE SZKOLEŃ

- Wykonawca zobowiązany jest do przekazania Zamawiającemu następującej dokumentacji szkoleniowej:
  - Programu danego szkolenia
  - Kopii certyfikatu lub zaświadczenia potwierdzającego uczestnictwo w szkoleniu wydanego uczestnikowi.
  - Kopii materiałów szkoleniowych oznaczonych zgodnie z wymogami programu Cyberbezpieczny Samorząd, o ile ich przekazanie jest dopuszczalne przez producenta danego oprogramowania (szkolenia autoryzowane). W przypadku, gdy jednostka autoryzująca szkolenie nie dopuszcza do przekazania dodatkowej kopii materiałów Wykonawca zobowiązany jest złożyć odpowiednie oświadczenie w tym zakresie.
  - Listy obecności uczestników szkolenia, a w przypadku szkoleń prowadzonych on-line, raport z platformy szkoleniowej potwierdzający listę uczestników szkolenia.
- Zamawiający oświadcza, że przedmiot zamówienia finansowany jest w ponad 70% ze środków Konkursu Grantowego pn. „Cyberbezpieczny Samorząd” Priorytet II: Zaawansowane usługi cyfrowe, Działanie 2.2. - Wzmocnienie krajowego systemu cyberbezpieczeństwa, Fundusze Europejskie na Rozwój Cyfrowy 2021-2027

Skotyszyn, dn. 17.12.2025 r.

**WÓJT**  
mgr Bogusław Kręcis