Výzva k podání nabídek, na kterou se nevztahuje postup pro zadávací řízení dle zákona č. 134/2016., o zadávání veřejných zakázek[1]

Číslo zakázky (bude doplněno MPSV při uveřejnění)	
Název zakázky	**Vzdělávání zaměstnanců – MERIT GROUP a.s.**
Druh zakázky (služba, dodávka nebo stavební práce)	**služba**
Datum vyhlášení výzvy k podání nabídek	**2. 8. 2018**
Registrační číslo projektu	CZ.03.1.52/0.0/0.0/15_021/0000053
Název projektu	**Podpora odborného vzdělávání zaměstnanců II**
Název / obchodní firma zadavatele	MERIT GROUP a.s.
Sídlo zadavatele	Březinova 136/7, Hodolany, 779 00 Olomouc
Osoba oprávněná jednat za zadavatele, její telefon a e-mailová adresa	Weigel Petr, statutární ředitel, petr.weigel@merit.cz, tel.: 737 262 070
IČ zadavatele / DIČ zadavatele	25344609 / CZ25344609
Kontaktní osoba zadavatele ve věci zakázky, její telefon a e-mailová adresa	Elner Lukáš, lukas.elner@merit.cz, tel.: 731 142 488
Lhůta pro podání nabídek	**13. 8. 2018 do 10:00**
Místo pro podání nabídek	Březinova 136/7, Hodolany, 779 00 Olomouc

Popis (specifikace) předmětu zakázky

Předmětem zakázky je zajištění realizace 5 vzdělávacích kurzů.

Zadavatel požaduje realizaci kurzů jako celku a zajištění závěrečné zkoušky. Zároveň stanovuje, že 1 vyučovací hodinou se rozumí 60 minut.

Kurzy musí probíhat prezenčně.

Školící agentura musí účastníkům školení v potřebném počtu pro každý kurz poskytnout výukové materiály.

U kurzů budou dodrženy minimální počty hodin výuky uvedené u jednotlivých kurzů.

Získané znalosti budou ověřeny lektorem závěrečnou zkouškou.

Součástí plnění je mj. vydání osvědčení o úspěšném absolvování kurzu.

Zadavatel umožňuje uchazeči zajistit požadované kurzy prostřednictvím subdodavatele.

Kurzy:

[1] Pole s povinnými náležitostmi výzvy jsou podbarvená.

Implementing Cisco Secure Access Solutions – 1 osoba, 40 hodin (39 hodin výuky +1 hodina zkoušky)

Obsah vzdělávací aktivity

Cílem školení je seznámit studenty s řešením TrustSec, vlastnostmi IEEE 802.1X protokolu a konfiguraci Identity Service Engine (ISE) pro řešení 802.1X. Kurz seznámí studenty s architekturou, komponenty a vlastnosti řešení TrustSec, které je možné implementovat do síťového prostředí na základě využití 802.1X a RADIUS protokolu. Seznámení s teorií i praktickou konfigurací Cisco Identity Services Engine (ISE). Cisco ISE platforma nahrazuje stávající Cisco Secure Access Control System (ACS) a Network Admission Control (NAC) server, které jsou typicky využívany pro ověřování uživatelů přistupujících do vnitřní sítě. Studenti budou implementovat IEEE 802.1X síťové služby na přepínačích Cisco Catalyst a Nexus a Cisco wireless produktech. Studenti po absolvování kurzu jsou schopni konfigurovat 802.1X řešení na Cisco přepínačích, Wireless Controller a ISE 1.2.

Osnova

1.den (8 hod.)

- Síťový koncept a komponenty nutné pro implementaci 802.1X (2 hod.)
- IEEE 802.1X standard (3 hod.)
- Autentizační protokol EAP (3 hod.)

2.den (8 hod.)

- Role RADIUS protokolu v 802.1X procesu (2 hod.)
- Konfigurace síťové infrastruktury (suplikant, přepínač, WLC, ISE, operační systém) (3 hod.)
- Konfigurace různých scénářů nasazení (MAB - MAC Authentication Bypass, webová autentizace, zařízení bez suplikanta, monitorovací režim, Low Impact ....) (3 hod.)

3.den (8 hod.)

- Guest Access, autorizace uživatelů, monitoring autentizovaných uživatelů (2 hod.)
- Design 802.1X pomocí Cisco ISE, kritické scénáře v důsledku výpadku (3 hod.)
- Seznámení s Cisco TrustSec 2.0 a ISE architekturou (3 hod.)

4.den (8 hod.)

- Možnosti nasazení Cisco Identity Services Engine - instalace Cisco ISE, konfigurace vysoké dostupnosti Cisco ISE (4 hod.)
- Klasifikace a politiky - využití Cisco ISE pro vynucení politik, konfigurace Cisco ISE pro MAB (MAC Authentication Bypass), konfigurace Cisco ISE pro wired a wireless 802.1X autentizaci, nasazení ISE do VPN prostředí, nasazení ISE s Web autentizací (4 hod.)

5.den (8 hod.)

- Guest, Profiler a Posture služby (3 hod.)
- Návrh Cisco TrustSec 2.0 architektury pro ISE (4 hod.)
- Závěrečná zkouška (1 hod.)

IT security technologies - 1 osoba, 56 hodin (54 hodin výuky +2 hodiny zkoušky)

Obsah vzdělávací aktivity

1.blok

Tento blok se soustředí na správu firewall boxů SRX založených na operačním systému Junos a jeho pokročilých funkcí jako jsou IPsec VPN, NAT, Screening, IDP apod.

Osnova

1.den (8 hod.)

Prvotní instalace (2 hod.)
- Nastavení z prostředí CLI
- Nastavení z prostředí Web UI
- Ověření konektivity a řešení problémů

Zóny (3 hod.)
- Potřeba zónování
- Konfigurace zón
- Monitoring

Bezpečnostní politiky (3 hod.)
- Popis politik
- Konfigurace politik
- Kontrola nastavení

2.den (8 hod.)

Autentizace uživatelů (3 hod.)
- Přehled AAA serverů
- Webová autentizace
- Klientské skupiny
- Konfigurace externích serverů
- Kontrola nastavení

Nastavení doplňkových funkcí (3 hod.)
- Ochrana na jednotlivých síťových vrstvách
- Typy útoků
- Nastavení UTM funkcí
- Kontrola nastavení

Překlady adres (2hod.)
- Přehled
- Cílový překlad adres
- Zdrojový překlad adres
- Proxy ARP
- Monitoring a kontrola správnosti překladů

3.den (8 hod.)

IPsec VPN (3 hod.)
- Typy VPN spojení
- Potřeby tunelování
- IPsec popis
- Konfigurace VPN
- Kontrola a monitoring

Junos IDP (2 hod.)
- Přehled funkce
- IDP politiky a komponenty
- Databáze útoků
- Příkladová studie

- Kontrola a monitoring

Řešení vysoké dostupnosti HA (2 hod.)

- Přehled funkce
- HA komponenty
- HA nastavení
- Monitoring HA

Závěrečná zkouška (1 hod.)

2.blok

V tomto bloku se účastník naučí navigaci v uživatelském rozhraní a vyšetřování útoků. Naučí se hledat a analyzovat informace, které software QRadar SIEM označí podezřelou činnost. Praktická cvičení posilují získané dovednosti

Osnova

1.den (8 hod.)

Unit 1: Úvod do IBM Security QRadar SIEM (1hod.)

Unit 2: Jak QRadar SIEM shromažďuje bezpečnostní data (2 hod.)

Unit 3: Použití panelu QRadar SIEM (1 hod.)

Unit 4: Vyšetřování útoku, který je vyvolán událostmi(2 hod.)

Unit 5: Vyšetřování okolností útoku (2 hod.)

2.den (8 hod.)

Unit 6: Používání aktivních profilů k vyšetřování útoků (2 hod.)

Unit 7: Vyšetřování útoku spuštěného toky (2 hod.)

Unit 8: Použití pravidel a stavebních bloků (1 hod.)

Unit 9: Vytváření reportů ze služby QRadar SIEM (1 hod.)

Unit 10: Pokročilé filtrování_(1 hod.)

Unit 11: Závěrečná zkouška (1 hod.)

3.blok

Dvoudenní blok pro pokročilé administrátory Zabbixu. Předmětem školení je výklad a praktické procvičení principů konfigurace a instalace monitorovacího systému Zabbix.

1.den (8 hod.)

- Úvod, Zabbix monitoringu – připomenutí **(1 hod.)**
- Výklad pojmů, principy konfigurace monitoringu – připomenutí **(1 hod.)**
- Interní procesy Zabbix, monitoring Zabbixu Zabbixem **(1 hod.)**
- Monitorování databází pomocí ODBC **(1 hod.)**

LAB 1a: Monitoring databází pomocí SQL dotazu (1 hod.)

- Rozšířené monitorování pomocí zabbix agent modulů
- Ukázky existujících GitHub projektů v jazyce C
- Popis kompilace modulů

LAB 1b: Monitoring MySQL/MariaDB pomoci mysql.so (1 hod.)

- Popis LLD pro jednotlivé instance MySQL
- Zabbix API a jeho možnosti
- Programovací jazyky a Zabbix API – JSON

LAB 1c: konfigurace uživatele využívajícího API (1 hod.)

LAB 1d: ukázka API – výpis monitorovaných hostů (1 hod.)

2.den (8 hod.)

- Monitoring pomoci IPMI – iDRAC **(1 hod.)**
- Nástroje projektu OpenIPMI **(1 hod.)**
- Konfigurace IPMI (iDRAC,iLO) pro realizaci monitoringu **(1 hod.)**

LAB 2a: sledování hardware (1 hod.)

- Monitoring Java aplikačních serverů pomocí JMX rozhraní
- Práce s nástrojem JConsole
- Definice JMX endpoints

LAB 2b: sledování JVM - Zabbix Java Gateway (1 hod.)

- Monitoring VMware infrastruktury
- Konfigurace VMware pro realizaci monitoring
- Monitoring VMware pomocí Perl VMware SDK

LAB 2c: monitorování VMware pomocí Perl API (1 hod.)

- Monitoring VMware pomocí zabbix_server

LAB 2d: konfigurace Zabbix nativního monitoringu VMware (1 hod.)

Závěrečná zkouška (1 hod.)

Scaling and optimalization of IT infrastructure – 1 osoba, 80 hodin (78 hodin výuky+2 hodiny zkoušky)

Obsah vzdělávací aktivity

1.blok

Během tohoto 5 denního bloku, účastník získá pokročilé znalosti, zkušenosti, postupy a možnosti k získání kompetencí během řešení problémů s komponentami View balíku VMware Horizon® 7. Zvýší si zkušenosti s používáním VMware nástrojů a nástrojů třetích stran k analýze a řešení problémů spojených s implementací VMware View. Tento prakticky intenzivní kurz vám poskytne rozsáhlé prostředí k ozkoušení svých znalostí během zjišťování a řešení širokého rozsahu případů.

Podrobný popis

Den 1 (8 hod.)

.1 Úvod do kurzu (2 hod.)
2. Úvod s odstraňováním problémů (3 hod.)
3. Nástroje pro odstraňování problémů (3hod.)

Den 2 (8 hod.)

4. Odstraňování problémů s virtuálními desktopy (8 hod.)

Den 3 (8 hod.)

5. Odstraňování problémů s připojením USB a tiskem (4 hod.)
6. Odstraňování problémů se zobrazovacími protokoly (4 hod.)

Den 4 (8 hod.)

7. Odstraňování problémů s View Composerem (4 hod.)
8. Odstraňování problémů s Instant Clones (4 hod.)

Den 5 (8 hod.)

9. Odstraňování problémů s SSL certifikáty (3 hod.)
10. Infrastruktura (4 hod.)
11. Závěrečná zkouška (1 hod.)

2.blok

IBM Spectrum Protect 8.1.2 je řešení pro zálohování a obnovu dat navržené tak, aby vám pomohlo spravovat uchovávání dat, snižovat náklady na ukládání dat a poskytovat přiměřené cíle bodů obnovy tak, aby byly splněny všechny dohody o úrovni služeb. IBM Spectrum Protect nabízí vylepšenou efektivitu a flexibilitu s využitím objektově řízeného řízení dat a udržování řízené politiky. Tento pětidenní kurz se zaměří na implementaci a základní správu prostředí IBM Spectrum Protect. Praktické laboratorní cvičení probíhají v prostředí W indows 2012. Materiály kurzu obsahují příklady příkazů AIX a Linux, které se liší od Windows

Osnova

1.den (8 hod.)

Unit 1: Komponenty a koncepty (4 hod.)

Unit 2: Instalace a konfigurace (4 hod.)

2.den (8 hod.)

Unit 3: Rozhraní a monitoring. (2 hod.)

Unit 4: Úložiště a zařízení (3 hod.)

Unit 5: Řízení zásad, pohyb dat a průzkum (3 hod.)

3.den (8 hod.)

Unit 6: Správa databáze serverů a databází úložiště. (4 hod.)

Unit 7: Konfigurace klienta (4 hod.)

4.den (8 hod.)

Unit 8: Ochrana dat klienta (4 hod.)

Unit 9: Denní provoz a údržba (4 hod.)

5.den (8 hod.)

Unit 10: Plány a reporty (7 hod.)

Závěrečná zkouška (1 hod.)

Konfigurace přepínačů a bezpečnost v sítích – 1 osoba, 64 hodin (62 hodin výuky+2 hodiny zkoušky)

Obsah vzdělávací aktivity

1.blok

Blok seznamuje účastníky se základními teoretickými a praktickými (konfiguračními) znalostmi o Cisco přepínačích používaných v ethernet LAN sítích. Jeho délka jsou tři dny tzn. 24 hodin. Po absolvování bloku bude účastník seznámen s produktovou řadou ethernet přepínačů, s nejpoužívanějšími technologiemi a funkcemi implementovanými v přepínačích. Většina teoretických statí je doplněna o konfigurační část.

Osnova

1.den (8 hod.)

- Přehled nejpoužívanějších Ethernet standardů (metalických a optických), stručný přehled kabeláže, konektorů a transceiverů (3 hod.)
- Adresace na druhé vrstvě OSI modelu, základní principy a funkce switchingu a Cisco přepínačů (3 hod.)
- Přehled aktuálních modelových řad přepínačů z rodiny Cisco Catalyst (2 hod.)

2.den (8 hod.)

- Ovládání IOS na Cisco přepínačích, základní konfigurační příkazy (2 hod.)
- Zabezpečení switchů - port security a bezpečný management (2 hod.)
- Virtuální lokální sítě (VLAN), Trunky - 802.1Q, Vlan Trunking Protocol (VTP) (2 hod.)
- Spaning Tree protocol, 802.1D - PVST+, 802.1w - RapidPVST+, stručný přehled dalších používaných protokolů (2 hod.)

3.den (8 hod.)

- L2 a L3 Etherchannel, principy fungování a jeho konfigurace (2 hod.)
- Možnosti směrování mezi VLAN (Inter VLAN routing, Multilayer switching) (3 hod.)
- Řešení redundance při směrování pomocí HSRP (Hot Standby Routing Protocol) a přehled dalších možností (3 hod.)

2.blok

Pětidenní blok navazující na detaily lokální bezpečnosti, který přináší informace o moderních podnikových zabezpečovacích technologiích na platformě Windows Server 2016.

Osnova

1.den (8 hod.)

Modul 1: Útoky, detekce porušení a nástroje Sysinternals (3 hod.)

- Pochopení útoků
- Zjišťování porušení
- Zkoumání aktivity pomocí nástroje Sysinternals
- Laboratoř: Základní strategie detekce poruch a reakce na incidenty
- Identifikace typů útoků
- Prozkoumáním nástrojů Sysinternals

Modul 2: Ochrana pověření a privilegovaný přístup (3 hod.)

- Porozumění uživatelským právům
- Počítačové a servisní účty
- Ochrana pověření
- Pracovní stanice s oprávněným přístupem a servery skoku
- Řešení místního správce-heslo

Modul 3: Omezení práv administrátora pomocí administrace Just Enough(2 hod.)

- Pochopení JEA
- Ověření a nasazení služby JEA

2.den (8 hod.)

Modul 4: Privilegované řízení přístupu a správní foresty (2 hod.)

- Foresty ESAE
- Přehled produktu Microsoft Identity Manager
- Přehled administrace JIT a PAM

Modul 5: Zmírnění malwaru a hrozeb(3 hod.)

- Konfigurace a správa systému Windows Defender
- Omezení softwaru
- Konfigurace a používání funkce Ochrana zařízení
- Nasazení a používání nástroje EMET

Modul 6: Analýza aktivity s pokročilým auditem a protokolovou analýzou (3 hod.)

- Přehled auditu
- Pokročilý audit
- Audit a protokolování systému Windows PowerShell

3.den (8 hod.)

Modul 7: Nasazení a konfigurace aplikace Advanced Threat Analytics a Microsoft Operations Management Suite (2 hod.)

- Nasazení a konfigurace ATA
- Nasazení a konfigurace aplikace Microsoft Operations Management Suite

Modul 8: Bezpečná virtualizační infrastruktura (3 hod.)

- Guarded Fabric
- Stíněné virtualizační přístroje podporující šifrování
- Lab: Guarded Fabric s certifikátem důvěryhodným administrátorem a stíněnými VM
- Nasazení chráněné fabric s potvrzením důvěryhodného správce
- Nasazení stíněného VM

Modul 9: Zabezpečení vývoje aplikací a infrastruktury serveru pro práci (3 hod.)

- Použití nástroje SCM
- Úvod do Nano serveru
- Pochopení kontejnerů

4.den (8 hod.)

Modul 10: Plánování a ochrana dat (2 hod.)

- Plánování a implementace šifrování
- Plánování a implementace nástroje BitLocker

Modul 11: Optimalizace a zabezpečení souborů služeb (3 hod.)

- Správce prostředků souborového serveru
- Provádění úkolů správy klasifikace a správy souborů
- Dynamické řízení přístupu

Modul 12: Zabezpečení síťového provozu s firewally a šifrováním (3 hod.)

- Pochopení bezpečnostních hrozeb souvisejících se sítí
- Chápání brány firewall systému Windows s pokročilým zabezpečením
- Konfigurace protokolu IPsec
- Datacenter Firewall

5.den (8 hod.)

Modul 13: Zabezpečení síťového provozu (5 hod.)

- Bezpečnostní hrozby související se sítí a pravidla zabezpečení připojení
- Konfigurace pokročilých nastavení DNS
- Zkoumání síťové komunikace pomocí analyzátoru zpráv Microsoft
- Zajištění provozu SMB a analýza provozu SMB

Modul 14: Aktualizace systému Windows Server (2hod.)

- Přehled služby WSUS
- Nasazení aktualizací pomocí služby WSUS

Závěrečná zkouška (1 hod.)

Nasazení a správa Windows a Office v podnikovém prostředí – 2 osoby, 80 hodin (78 hodin výuky +2 hodiny zkoušky)

Obsah vzdělávací aktivity

1.blok

Cílem bloku, který trvá 40 hodin, tzn. 5 dní, je seznámit účastníka se založením Office 365, s naplánováním a nasazením síťové připojení k Office 365, se spravováním uživatelských účtů v cloudu, se spravováním uživatelských účtů pomocí DirSync, s řízením přístupů pomocí AD FS, se sledováním využití cloudových služeb a řešením potíží s přístupem, se spravováním licence a koncových zařízení uživatelů, s vytvářením kolekce webů SharePoint Online, s plánováním a nasazením Exchange Online a Lync Online služby

Osnova

1.den

- Plánování a porozumění technologii Office 365
- Vytváření zákaznických účtů (tenant)
- Zajištění konektivity klientů a jejich síťových parametrů
- Správa uživatelů a licencí
- Správa bezpečnostních skupin a distribučních seznamů
- Správa účtů pomocí Windows PowerShell skriptů

2.den

- Řízení rolí správců v prostředí cloudu
- Správa hesel a jejich zásady
- User-driven nasazení a připojení klientských zařízení
- Podnikové nasazení Office 365 ProPlus
- Telemetrie, sledování výkonu a výstupy sestav
- Vlastní emailové domény, jejich vytváření a správa

3.den

- Doporučené postupy migrace mailboxů do cloudového prostředí
- Sdílení s externími uživateli
- Plánování Exchange Online služeb
- DNS záznamy pro Exchange Online
- Osobní archivační zásady
- Emailové adresy uživatelů
- Externí kontakty, prostředky a skupiny

4.den

- Správa kolekcí webů v SharePoint Online
- Externí přístup do SharePoint Online
- Plánování prostředí SharePoint Online
- Nastavení Lync Online
- Příprava firemního Active Directory pro spolupráci s cloudem

5.den

- Nastavení DirSync
- Synchronizace účtů pomocí DirSync a jejich správa v kombinaci s cloudem
- Plánování AD FS ověřování
- Zjištění a řešení výpadků služeb
- Sledování zdraví služeb
- Vytváření sestav výsledků sledování
- Závěrečná zkouška (1 hod.)

2.blok

Pětidenní blok pro pokročilejší správce Windows 10, kteří se chtějí seznámit s podrobnostmi centrálního nasazení a správy stanic a virtuálních stanic pomocí Group Policy a cloud technologie Windows Intune v podnikovém prostředí.

Co se v kurzu účastník naučí:

- Nasadit Windows 10 stanice do podnikového prostředí
- Spravovat uživatelské profily a nastavení
- Spravovat přihlašovací identity a účty
- Použít Group Policy ke správě uživatelského prostředí a bezpečnosti
- Řídit přístup na data
- Spravovat a nasadit vzdálený přístup
- Používat klientské Hyper-V
- Spravovat zařízení s Windows 10 pomocí Enterprise Mobility Suite
- Spravovat klientská zařízení pomocí Intune
- Aktualizovat Windows 10 přes Intune
- Spravovat aplikace pomocí Intune

Osnova

1.den (8 hod.)

- Správa Windows 10 v podnikovém prostředí (2 hod.)
- Správa mobilních zařízení (1 hod.)
- Podpora zařízení a desktopů (1 hod.)
- Cloudové služby (1 hod.)
- Nasazení klientů v podnikovém prostředí(2 hod.)
- Příprava a úprava obrazů operačních systémů a parametrů nasazení (1 hod.)

2.den (8 hod.)

- Microsoft Deployment Toolkit (1 hod.)
- Správa instalací s Windows 10 (1 hod.)
- Aktivace a licencování a správa volume licensing(1 hod.)
- Uživatelské profily a nastavení(1 hod.)
- Group Policy a User State Virtualization(1 hod.)
- User Experience Virtualization (1 hod.)
- User State Migration(1 hod.)
- Přehled možností ověřování a uživatelských účtů(1 hod.)

3.den (8 hod.)

- Cloud Identity Integration (1 hod.)
- Správa Group Policy objektů (0,5 hod.)
- Konfigurace stanic pomocí GPO (1 hod.)
- Group Policy Preferences (1 hod.)
- Řízení přístupu k datům (0,5 hod.)
- Registrace zařízení (1 hod.)
- Work Folders (0,5 hod.)
- Data v cloudu a přístup k nim (1 hod.)
- Vzdálený přístup (0,5 hod.)
- Konfigurace vzdáleného přístupu (1 hod.)

4.den (8 hod.)

- DirectAccess (1 hod.)
- Podpora pro RemoteApp (1 hod.)
- Klientské Hyper-V (1 hod.)
- Virtuální switche s sítě (1 hod.)
- Virtuální disky (1 hod.)
- Virtuální počítače Přehled Enterprise Mobility Suite (EMS) (1 hod.)
- Přehled Azure Active Directory Premium (AAD) (1 hod.)
- Přehled Azure Rights Management (RMS) (1 hod.)

5.den (8 hod.)

- Přehled Microsoft Intune (1 hod.)

• Distribuce klientů Intune (0,5 hod.) • Přehled centrálních Intune Policies (0,5 hod.) • Intune a Mobile Device Management (1 hod.) • Aktualizace operačních systémů přes Intune (1 hod.) • Endpoint Protection (0,5 hod.) • Správa aplikací pomocí Intune (1 hod.) • Nasazení aplikací pomocí Intune(0,5 hod.) • Řízení přístupu na podnikové prostředky (1 hod.) • Závěrečná zkouška (1 hod.)

Předpokládaná hodnota zakázky v Kč (bez DPH)	**451.450,- Kč bez DPH** Celková cena zakázky nesmí překročit předpokládanou hodnotu. Zadavatel stanoví cenu jako maximální, nepřekročitelnou. Překročení ceny povede k vyřazení nabídky.
Lhůta dodání / časový harmonogram plnění / doba trvání zakázky	srpen 2018 – červenec 2019
Místo dodání / převzetí plnění	Praha, Brno, Ostrava

Pravidla pro hodnocení nabídek, která zahrnují i) kritéria hodnocení, ii) metodu vyhodnocení nabídek v jednotlivých kritériích a iii) váhu nebo jiný matematický vztah mezi kritérii

- Nabídková cena bez DPH (40 %) – číselné kritérium

  Dodavatel je povinen stanovit celkovou nabídkovou cenu za předmět plnění veřejné zakázky absolutní částkou v českých korunách v členění na cenu s a bez DPH. Hodnocena přitom bude celková nabídková cena bez DPH. Z důvodu požadavku na nepřekročení předpokládaných hodnot uvede dodavatel v nabídce ceny za jednotlivé aktivity.

- Metodika organizace kurzů (60 %) – nečíselné kritérium

  Tímto kritériem se myslí dokument, který v rozsahu maximálně 10 stran popíše postup uchazeče k plnění předmětu veřejné zakázky. Hodnoceny budou způsoby realizace pro Zadavatele klíčových částí požadovaného plnění, které dodavatel v Metodice organizace kurzů popíše, a které se budou vztahovat k efektivitě výuky. Konkrétně bude hodnocen popis:

  a) metodiky výuky,

  b) efektivity výukových metod,

  c) způsobu ověřování kvality výuky a získávání zpětné vazby;

  d) systematičnost nabízených služeb;

  e) efektivní způsob realizace zakázky.

  Lépe bude hodnocen dodavatel, který nabídne efektivnější a pro Zadavatele ověřitelnější způsob organizace kurzů. Lépe bude hodnocen dodavatel, který bude reagovat na potřeby aktuální cílové skupiny. Dále bude lépe hodnocen dodavatel, který zajistí efektivnější proces zahrnující způsob organizace zakázky včetně akceptace plnění a komunikace se zadavatelem a účastníky vzdělávání.

Pro hodnocení budou využity následující metody:

hodnota z nabídky, která je v daném kritériu nejvýhodnější tzn. nejnižší hodnota (Nabídková cena bez DPH)

100 x ---------- x váha kritéria vyjádřená v %

hodnota (např. cena) z hodnocené nabídky

Pro hodnocení subjektivních (nečíselných) kritérií se použije bodová stupnice 1 ž 100. Nejvhodnější nabídce je vždy přiřazena hodnota 100 bodů, ostatním jsou přiřazeny body odpovídající výsledku jejich porovnání s touto nejvhodnější nabídkou v daném kritériu.

počet bodů, které hodnocená nabídka x váha kritéria vyjádřená v % v daném kritériu získala

Takto získané vážené body ze všech dílčích hodnoticích kritérií se sečtou. Nabídka, která získala v součtu za všechna hodnocená kritéria nejvíce bodů, je nabídkou vítěznou.

Hodnocení nabídek proběhne v souladu s pravidly uvedenými v Obecné části pravidel pro žadatele a příjemce v rámci OP Zaměstnanost v kapitole Pravidla pro zadávání zakázek.

Požadavky na prokázání kvalifikace dodavatele

1. Základní způsobilost:

Uchazeč musí prokázat splnění základní způsobilosti stanovené analogicky s § 74 zákona o zadávání veřejných zakázek. Splnění základních způsobilosti prokáže uchazeč předložením dokumentů stanovených v § 75 zákona o zadávání veřejných zakázek, a to v prosté kopii.

2. Profesní způsobilost:

Způsobilý je uchazeč, který předloží:

- výpis z obchodního rejstříku, pokud je v něm zapsán, či výpis z jiné obdobné evidence, pokud je v ní zapsán;
- doklad o oprávnění k podnikání podle zvláštních právních předpisů v rozsahu odpovídajícím předmětu veřejné zakázky, zejména doklad prokazující příslušné živnostenské oprávnění či licenci, a to v minimálně:
    - Výroba, obchod a služby neuvedené v přílohách 1 až 3 živnostenského zákona.

Doklady prokazující splnění základní způsobilosti a výpis z obchodního rejstříku musí prokazovat splnění požadovaného kritéria způsobilosti nejpozději v době 3 měsíců přede dnem zahájení výběrového řízení.

Namísto předložení dokumentů požadovaných zadavatelem je dodavatel oprávněn prokázat svou kvalifikaci výpisem ze seznamu kvalifikovaných dodavatelů (obdobně podle § 228 zákona o zadávání veřejných zakázek) nebo certifikátem vydaným v rámci systému certifikovaných dodavatelů (obdobně podle § 239 zákona č. 134/2016 Sb.).

Dodavatel předloží seznam významných služeb (ve formě čestného prohlášení) poskytnutých za poslední 3 roky před zahájením výběrového řízení včetně uvedení ceny a doby jejich poskytnutí a identifikace objednatele, ze kterého bude vyplývat, že řádně a odborně poskytl alespoň tři služby, jejichž předmětem bylo zajištění vzdělávání dospělých. Každá ze služeb musí mít hodnotu min. 230.000 Kč bez DPH.

Dodavatel doloží kvalifikaci alespoň 2 lektorů, přičemž lektoři budou mít dále uvedenou kvalifikaci (v souhrnu, nikoliv nutně každý samostatně). Požadovaný certifikát lektora musí být součástí nabídky.

- CCNP (Cisco Certified Network Professional) Security nebo Routing a Switching
- VMware (VMware Certified Instructor)
- Microsoft (Microsoft Certified Trainer)

Je postačující, aby výše uvedené podklady prokazující splnění kvalifikace byly předloženy v podobě kopií, nestanoví-li zadavatel ve výzvě k podání nabídek jinak.

Podmínky a požadavky na zpracování nabídky

Dodavatel je povinen předložit návrh smlouvy.

Návrh smlouvy musí být podepsán dodavatelem či osobou jednající na základě plné moci od statutárního orgánu.

Smlouva musí mít písemnou formu a musí obsahovat alespoň tyto náležitosti:

- Identifikační údaje smluvních stran včetně IČ a DIČ, pokud jsou přiděleny
- Předmět plnění (konkretizovaný kvantitativně a kvalitativně)
- Cenu bez DPH a informaci, zda dodavatel je či není plátcem DPH
- Platební podmínky
- Lhůtu dodání nebo harmonogram plnění
- Místo dodání/převzetí zboží nebo výstupu plnění (není-li výslovně sjednáno, rozumí se jím sídlo zadavatele)
- Závazek dodavatele předkládat k proplacení pouze faktury, které obsahují název a číslo projektu
- Zapracování údajů z nabídky, které byly předmětem posouzení/hodnocení kvalifikace (tj. v okamžiku uzavření smlouvy i během realizace zakázky musí obsah smluvního vztahu odpovídat alespoň těm parametrům nabídky, které zadavatel posuzoval nebo hodnotil).

Celá nabídka bude zpracována v českém jazyce. Dokumenty v cizím jazyce budou opatřeny překladem do českého jazyka (nevztahuje se na certifikáty lektorů vystavené v anglickém jazyce).

Požadavek na způsob zpracování nabídkové ceny	Dodavatel zpracuje nabídkovou cenu na samostatném listu nabídky a uvede ji jako celkovou cenu za realizaci předmětu veřejné zakázky v členění cena bez DPH, samostatně DPH a cena včetně DPH. Z důvodu úhrady po jednotlivých kurzech uvede také ceny jednotlivých kurzů.
Požadavek na písemnou formu nabídky	Nabídka musí být zadavateli podána v listinné podobě v řádně uzavřené obálce označené názvem zakázky a nápisem „Neotevírat“, na níž je uvedena kontaktní adresa uchazeče. Nabídky musí být podepsány dodavatelem či osobou oprávněnou zastupovat dodavatele.[2]
Požadavek na uvedení kontaktní osoby dodavatele	Dodavatel ve své nabídce uvede kontaktní osobu ve věci zakázky, její telefon a e-mailovou adresu.
Požadavek na jednu nabídku	Každý dodavatel může podat pouze jednu nabídku.

Vysvětlení zadávacích podmínek

Dodavatel je oprávněn po zadavateli požadovat vysvětlení zadávacích podmínek (odpovědi na dotaz). Písemná žádost musí být zadavateli doručena nejpozději 4 pracovní dny před uplynutím lhůty pro podání nabídek.

Další požadavky na zpracování nabídky

Platební podmínky:

- Úhrada bude prováděna na měsíční bázi podle již počtu realizovaných kurzů. Faktury budou vystavovány s min. 15 denní splatností.
- Možnost navýšení ceny v objektivně daných případech (pouze změna ceny v závislosti na případné změně výše DPH)

Další obchodní podmínky:

- Dodavatel bude ve smlouvě zavázán povinností umožnit osobám oprávněným k výkonu kontroly projektu, z něhož je zakázka hrazena, provést kontrolu dokladů souvisejících s plněním zakázky, a to po dobu danou právními předpisy ČR k jejich archivaci (zákon č. 563/1991 Sb., o účetnictví, a zákon č. 235/2004 Sb., o dani z přidané hodnoty).

Požadavky na formu nabídky:

- Zadavatel požaduje předložení nabídky v 1 originálním vyhotovení.
- Zadavatel nepřipouští variantní řešení nabídek.

[2] Osobou oprávněnou jednat za dodavatele se rozumí osoba jednající na základě plné moci od statutárního orgánu.

Zadávací řízení se řídí	Obecnou částí pravidel pro žadatele a příjemce v rámci Operačního programu Zaměstnanost (vydání č. 8), na toto zadávací řízení se neaplikují ustanovení zákona č. 134/2016 Sb., o zadávání veřejných zakázek.
Dodavatelé budou vyrozumíváni o výsledku, resp. zrušení zadávacího řízení a o příp. vyloučení nabídky prostřednictvím uveřejnění informace na portálu www.esfcr.cz pod výše uvedeným názvem veřejné zakázky.	

Datum a podpis osoby oprávněné jednat za zadavatele	V Olomouci dne 26. 7. 2018