MĚSTO Dobruška

Objednávka č. DO00169

Alpiro, s. r. o.
Piletická 486
503 41 HRADEC KRÁLOVÉ
IČO: 24156426
DIČ: CZ24156426

Datum: 16.03.2026

Objednáváme u Vás:

vypracování výstupního auditu kybernetické bezpečnosti dle požadavků poskytovatele dotace pro projekt „Rozvoj kybernetické bezpečnosti města Dobrušky“, registrační číslo projektu CZ.31.2.0/0.0/0.0/23_093/0008372, v rozsahu popsaném v příloze této objednávky „Výstupní audit kybernetické bezpečnosti – specifikace činností“ za cenu **265.000,00 Kč bez DPH, tj. 320.650,00 Kč vč. DPH 21 %.**

Termín pro vyřízení:
Do **15.05.2026.**

Odešlete na naši adresu: Město Dobruška, Solnická 777, 518 01 Dobruška
Kontaktní osoba: Martin Pošvář, mobil: [redacted], e-mail: [redacted]

Fakturační adresa:
Město Dobruška, Solnická 777, 518 01 Dobruška
IČO: 00274879, DIČ: CZ00274879
Bankovní spojení: Komerční banka, č. účtu 1721571/0100

K faktuře přiložte jeden výtisk objednávky nebo její kopii. Ve faktuře uveďte číslo této objednávky! Součástí faktury nebo v příloze bude uveden soupis provedených prací nebo rozpis dodávky.

Město Dobruška je plátcem DPH.

Město zdanitelné plnění ~~**použije**~~ / **nepoužije* pro svou ekonomickou činnost,** kdy se podle zákona o dani z přidané hodnoty považuje za osobu povinnou k dani ve vztahu k danému plnění.

~~Uplatní~~ / neuplatní* režim PDP
Při uplatnění režimu přenesené daňové povinnosti u stavebních a montážních prací vystaví dodavatel fakturu **bez uvedení sazby a výše DPH se sdělením „daň odvede zákazník“.** (podle § 92 odst. 2, písm. c zákona o DPH)

* nehodící se škrtněte

Razítko a podpis odpovědného pracovníka:

_____
Mgr. Martin Vídeňský, vedoucí odboru majetku a investic

Podpis správce rozpočtu:

_____
Ing. Klára Škopová, DiS., vedoucí odboru finančního a školského

Akceptace objednávky:

Datum: _____18.03.2026_____

Jméno, příjmení a funkce oprávněné osoby _____

Podpis oprávněné osoby: Mgr. Karel Rejent
_____

Výstupní audit kybernetické bezpečnosti – specifikace činností a podmínek

Výstupní audit kybernetické bezpečnosti (dále jen „audit“) představuje nezávislé a objektivní posouzení kybernetického zabezpečení organizace. Cílem auditu je identifikace slabých míst v infrastruktuře a ověření shody nastavených opatření s aktuálně platnou legislativou v oblasti kybernetické bezpečnosti a s požadavky poskytovatele dotace na projekt „Rozvoj kybernetické bezpečnosti města Dobrušky“, registrační číslo projektu CZ.31.2.0/0.0/0.0/23_093/0008372.

1. Metodika a legislativní rámec

Audit je realizován v souladu s následujícími předpisy a normami:

- **Zákon č. 264/2025 Sb.**, o kybernetické bezpečnosti.
- **Vyhláška č. 410/2025 Sb.**, o bezpečnostních opatřeních poskytovatele regulované služby v režimu nižších povinností.
- **Směrnice NIS2** a **ENISA ECSF** (European Cybersecurity Skills Framework).
- Standardy řady **ISO/IEC 27000**.

2. Rozsah auditu

Předmětem auditu jsou následující oblasti:

- **Síťová infrastruktura:** Zabezpečení perimetru (firewall), kontrola zabezpečení vnitřní sítě, kontrola segmentace a zabezpečení bezdrátových sítí.
- **Koncová zařízení a servery:** Bezpečnost operačních systémů a nastavení antivirové ochrany.
- **Identita a přístup:** Zabezpečení doménové infrastruktury, správa administrátorských účtů a politika hesel.
- **Záloha dat a kontinuita činnosti:** Kontrola nastavení záloh, kontrola zabezpečení souborů záloh a ověření dostupnosti služeb.
- **Komunikace a logování:** Zabezpečení elektronické pošty a kontrola nastavení logování bezpečnostních událostí.
- **Fyzická a organizační bezpečnost:** Fyzická bezpečnost IT infrastruktury a úroveň školení kybernetické bezpečnosti.

3. Požadavky na součinnost objednatele

- přístup (dálkový, případně i fyzický, a to výhradně v pracovní době městského úřadu a po předchozí domluvě),
- nepřímé zapojení (zodpovídání dotazů).

4. Povinnosti dodavatele

- dodavatel je povinen zahájit provádění auditu bez zbytečného odkladu po vystavení objednávky,
- dodavatel je při provádění auditu povinen postupovat pečlivě, dle svých nejlepších znalostí a schopností, přičemž je při své činnosti povinen sledovat a chránit oprávněné zájmy objednatele a

postupovat v souladu s jeho pokyny a dle platných dotačních pravidel pro výzvu č. 41 NPO „Kybernetická bezpečnost – obce“,

- dodavatel je povinen zajistit utajení důvěrných informací získaných při plnění objednávky způsobem obvyklým pro utajování takových informací, není-li výslovně sjednáno jinak; tato povinnost platí i po splnění objednávky,
- dodavatel se výslovně zavazuje chránit a zachovávat mlčenlivost o všech datech získaných nebo přístupných v informačním systému objednatele nebo i jinak, zejména o osobních údajích ve smyslu NAŘÍZENÍ EVROPSKÉHO PARLAMENTU A RADY (EU) 2016/679 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů) ze dne 27. dubna 2016 a utajovaných skutečnostech podle zákona č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti a o bezpečnostních opatřeních, jejichž zveřejnění by ohrozilo zabezpečení osobních údajů; dodavatel se zavazuje takové informace nezneužít ve svůj prospěch nebo ve prospěch jiného.

5. Výstupy auditu

Proces je zakončen předáním auditní zprávy v elektronické podobě v PDF a na žádost objednatele i 1x v tištěné podobě.

Výstupní audit kybernetické bezpečnosti – specifikace činností a podmínek

Výstupní audit kybernetické bezpečnosti (dále jen „audit“) představuje nezávislé a objektivní posouzení kybernetického zabezpečení organizace. Cílem auditu je identifikace slabých míst v infrastruktuře a ověření shody nastavených opatření s aktuálně platnou legislativou v oblasti kybernetické bezpečnosti a s požadavky poskytovatele dotace na projekt „Rozvoj kybernetické bezpečnosti města Dobrušky“, registrační číslo projektu CZ.31.2.0/0.0/0.0/23_093/0008372.

1. Metodika a legislativní rámec

Audit je realizován v souladu s následujícími předpisy a normami:

- **Zákon č. 264/2025 Sb.**, o kybernetické bezpečnosti.
- **Vyhláška č. 410/2025 Sb.**, o bezpečnostních opatřeních poskytovatele regulované služby v režimu nižších povinností.
- **Směrnice NIS2** a **ENISA ECSF** (European Cybersecurity Skills Framework).
- Standardy řady **ISO/IEC 27000**.

2. Rozsah auditu

Předmětem auditu jsou následující oblasti:

- **Síťová infrastruktura:** Zabezpečení perimetru (firewall), kontrola zabezpečení vnitřní sítě, kontrola segmentace a zabezpečení bezdrátových sítí.
- **Koncová zařízení a servery:** Bezpečnost operačních systémů a nastavení antivirové ochrany.
- **Identita a přístup:** Zabezpečení doménové infrastruktury, správa administrátorských účtů a politika hesel.
- **Záloha dat a kontinuita činnosti:** Kontrola nastavení záloh, kontrola zabezpečení souborů záloh a ověření dostupnosti služeb.
- **Komunikace a logování:** Zabezpečení elektronické pošty a kontrola nastavení logování bezpečnostních událostí.
- **Fyzická a organizační bezpečnost:** Fyzická bezpečnost IT infrastruktury a úroveň školení kybernetické bezpečnosti.

3. Požadavky na součinnost objednatele

- přístup (dálkový, případně i fyzický, a to výhradně v pracovní době městského úřadu a po předchozí domluvě),
- nepřímé zapojení (zodpovídání dotazů).

4. Povinnosti dodavatele

- dodavatel je povinen zahájit provádění auditu bez zbytečného odkladu po vystavení objednávky,
- dodavatel je při provádění auditu povinen postupovat pečlivě, dle svých nejlepších znalostí a schopností, přičemž je při své činnosti povinen sledovat a chránit oprávněné zájmy objednatele a postupovat v souladu s jeho pokyny a dle platných dotačních pravidel pro výzvu č. 41 NPO „Kybernetická bezpečnost – obce“,

- dodavatel je povinen zajistit utajení důvěrných informací získaných při plnění objednávky způsobem obvyklým pro utajování takových informací, není-li výslovně sjednáno jinak; tato povinnost platí i po splnění objednávky,
- dodavatel se výslovně zavazuje chránit a zachovávat mlčenlivost o všech datech získaných nebo přístupných v informačním systému objednatele nebo i jinak, zejména o osobních údajích ve smyslu NAŘÍZENÍ EVROPSKÉHO PARLAMENTU A RADY (EU) 2016/679 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů) ze dne 27. dubna 2016 a utajovaných skutečnostech podle zákona č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti a o bezpečnostních opatřeních, jejichž zveřejnění by ohrozilo zabezpečení osobních údajů; dodavatel se zavazuje takové informace nezneužít ve svůj prospěch nebo ve prospěch jiného.

5. Výstupy auditu

Proces je zakončen předáním auditní zprávy v elektronické podobě v PDF a na žádost objednatele i 1x v tištěné podobě.