Příloha č. 1

**Technická specifikace**

k veřejné zakázce na dodávky s názvem:

**„Dodávka HW zařízení a SW aplikací – Městský úřad Trutnov“**

1. **Identifikační údaje zadavatele**

|  |  |
| --- | --- |
| Název: | Město Trutnov |
| Sídlo: | Slovanské náměstí 165, 541 01 Trutnov |
| Zastoupený: | Ing. arch. Michal Rosa, starosta města |
| IČO: | 00278360 |

1. **Identifikace účastníka**

|  |  |
| --- | --- |
| Název: | …………………………………… |
| Sídlo: | …………………………………… |
| Osoba oprávněná za účastníka jednat: | …………………………………… |
| IČO: | …………………………………… |

1. **Předmět veřejné zakázky – technická specifikace HW zařízení a SW aplikací**
	* + 1. **UPS záložní zdroj pro diskové pole – 1 ks**
* Výstupní výkon minimálně 6kW/6kVA
* Výstupy minimálně:
* 1x Hard wire 3-wire (H N + E) (Battery Backup)
* 2x IEC Jumpers (Battery Backup)
* 4x IEC 320 C19 (Battery Backup)
* 1x Hard Wire 3-wire (H N + G) (Battery Backup)
* 6x IEC 60320 C13 (Battery Backup)
* Vstupní napětí 230V 50/60Hz +/- 3%
* Výstupní napětí 230V
* Vstupní konektor: Hard wire 3-wire (1P + N + E)
* Technologie online s dvojitou konverzí
* Bypass součástí
* Porty: 1x RJ-45 10/100 Base-T, 1x RJ-45 seriál port, Smart slot, USB
* Výška maximálně 4U, provedení do racku
* Včetně komunikační karty a plné licence pro management UPS
* Multifunkční LCD displej a kontrolní konzolí

3 roky záruka, včetně záruky na baterii

1. **Síťová infastruktura (páteřní switch vč. příslušenství) - 2 ks**

**Základní vlastnosti:**

* Třída zařízení: L3 switch
* Formát zařízení do racku
* Velikost zařízení: 1U
* Minimální počet 10GE optických portů s volitelným fyzickým rozhraním: 24x 10 Gbps SFP/SFP+
* Počet optických 10/25/50GE portů s volitelným fyzickým rozhraním: 4x 10/25/50 Gbps SFP/SFP+/SFP28/SFP56
* 2x interní hot-swap AC napájecí zdroj
* Vyměnitelné ventilátory – hot swap
* Celková propustnost přepínače minimálně: 880 Gbps
* Celkový paketový výkon přepínače minimálně: 654 Mpps
* Paketový buffer 8MB
* Maximální hloubka přepínače: 39 cm

**Vlastnosti stohování**

* Podporovaný počet přepínačů ve stohu: 10ks
* Kapacita stohovacího propojení: 200 Gbps
* Stoh podporuje distribuované přepínaní paketů
* Kterýkoli prvek ve stohu může být řídícím prvkem (1:N redundance)
* Jednotná konfigurace stohu (IP adresa, správa, konfigurační soubor)
* Seskupení portů IEEE 802.3ad mezi různými prvky stohu (Multichassis LAG)
* Stoh funguje jako jedno L3 zařízení (router, gateway, peer) včetně podpory dynamických směrovacích protokolů jako je OSPF

**Základní funkce a protokoly**

* Podpora "jumbo rámců" včetně velikosti 9198 Byte
* Podpora linkové agregace IEEE 802.1AX
* Konfigurovatelné rozkládání LACP zátěže podle L2,L3
* Počet LACP skupin/linek ve skupině: 256/8
* Počet záznamů v tabulce MAC adres minimálně: 32.000
* Počet záznamů v tabulce ARP minimálně: 49.000
* Protokol pro definici šířených VLAN: MVRP
* Podpora VLAN podle IEEE 802.1Q, minimálně 4000 aktivních VLAN
* VLAN translace - swap 802.1Q tagů na trunk portu
* Podpora zařazování do VLAN podle standardu 802.1v
* IEEE 802.1s - Multiple Spanning Tree
* STP instance per VLAN s 802.1Q tagováním BPDU (např. PVST+)
* Detekce protilehlého zařízení pomocí LLDP a rozšíření LLDP-MED
* Detekce jednosměrnosti optické linky (např. UDLD)
* DHCP server
* DHCP relay pro IPv4 a IPv6
* Podpora NTPv4 pro IPv4 a IPv6 včetně VRF a MD5 autentizace
* Statické směrování IPv4 a IPv6
* Počet záznamů ve směrovací tabulce: minimálně 61.000
* Dynamické směrování OSPFv2, OSPFv3 a BGP včetně podpory BFD
* Podpora BGP a MP-BGP včetně podpory BFD
* Podpora Layer-3 routed port
* IGMP v2 a v3
* MLD v1 a v2
* Hardware podpora IPv4 a IPv6 ACL
* ACL definice na základě skupiny fyzických portů
* ACL aplikovatelný na interface, LAG, VLAN
* BPDU a Root guard
* DHCP snooping pro IPv4 a IPv6
* HW ochrana proti zahlcení portu (broadcast/multicast/icmp) nastavitelná na kbps a pps
* 802.1X ověřování včetně více současných uživatelů na port, minimálně 32 uživatelů/port
* Konfigurovatelná kombinace pořadí postupného ověřování zařízení na portu (IEEE 802.1x, MAC adresou)
* Dynamické zařazování do VLAN a přidělení QoS podle RFC 4675
* Podpora Critical VLAN
* Podpora uživatelských rolí definujících pro konkrétní uživatele více tagovaných či netagovaných VLAN, ACL, QoS politiky a SDN tunely.
* Uživatelské role mohou být lokálně definované v přepínači nebo mohou být dynamicky stáhnuty z RADIUS serveru na základě výsledku autorizace.
* Podpora IPv6 RA Guard
* IP source guard / dynamic IP lockdown
* Podpora Dynamic ARP protection
* Port security
* Konfigurovatelná ochrana control plane (CoPP) před DoS útoky na CPU
* Podpora IPv4 a IPv6 QoS
* IEEE 802.1p - minimální počet front: 8

**SDN funkce**

* Podpora service insertion včetně technologie VXLAN
* Podpora BGP EVPN s využítím VXLAN
* Podpora tunelování uživatelského provozu pomocí L2 GRE tunelů - schopnost izololovat více koncových zařízení na jednom portu do unikátních tunelů
* Přiřazení koncového zařízení do tunelu na základě výsledku autorizace
* Analytické a automatizační nástroje
* Podpora REST API pro automatizaci nastavení sítě.
* Podpora skriptování v jazyce Python – lokální interpret jazyka v přepínači
* Integrovaný nástroj na odchyt paketů (např. WireShark nebo ekvivalentní)
* Interpretace uživatelských skriptů monitorujících definované parametry síťového provozu s možností automatické reakce na události
* Grafické rozhraní pro vynášení výsledků monitorování a analytických skriptů. Možnost vynášení stavu monitorovaných metrik do grafů atp.
* Root cause analysis v grafickém rozhraní – možnost vrácení se ke konkrétní funkční konfiguraci a stavu protokolů v čase.
* Interní uložistě dat pro sběr provozních dat a pokročilou dignostiku zařízení
* Kapacita interního úložiště dat pro analytické účely: 30 GB

**Management**

* USB-C konzolový port
* 1xRJ45 OoB management port s podporou ethernetu
* Podpora minimálně 64 virtuálních směrovacích instancí (VRF)
* Minimální počet VRF instancí: 64
* Konfigurace zařízení v člověku čitelné textové formě
* Podpora automatických i manuálních snapshotů konfigurace systému
* USB port pro diagnostiku, přenos konfigurace a firmware
* Přímé bezdrátové připojení ke konzoli zařízení skrze bluetooth
* Podpora managementu přes IPv4 i IPv6
* SSHv2 a HTTPS pro IPv4 a IPv6
* Podpora SNMPv2c a SNMPv3
* RMON
* Možnost omezení přístupu k managementu (SSH, SNMP) pomocí ACL
* Lokálně vynucené RBAC na úrovni přepínače
* Dualní flash image
* Podpora UDP, TCP a TLS SYSLOG pro IPv4 a IPv6 s možností logováni do více syslog serverů
* Podpora RADIUS včetně RADIUS CoA (RFC3576)
* Podpora TACACS+
* Analýza síťového provozu sFlow podle RFC 3176
* Port mirroring, alespoň 4 různé obousměrné session: SPAN, ERSPAN
* Podpora IP SLA pro měření zpoždění provozu VoIP
* Podpora Zero Touch Provisioning (ZTP)

**Ostatní podmínky:**

* Hardware musí být dodán zcela nový, plně funkční a kompletní (včetně příslušenství)
* Dodávka musí obsahovat veškeré potřebné licence pro splnění požadovaných vlastností a parametrů.
* Je požadována záruka na hardware s výměnou v délce 36 měsíců. Tato záruka musí být garantovaná výrobcem zařízení.
* Uchazeč je povinen s dodávkou doložit oficiální potvrzení lokálního zastoupení výrobce o všech dodávaných zařízeních (seznam sériových čísel dodávaných zařízení) pro český trh.

**Příslušenství:**

* 8ks 10G SFP+ LC SR 300m OM3 MMF Transceiver pro switche
* 2ks SFP+ transceiver 10Gbps, 10GBASE-T, do 30m (CAT 6A či 7), RJ-45 pro switche
* 6ks SFP+ transceiver 10GBASE-SR/SW, MM, LC dup., pro servery
* 2ks Optický patch kabel duplex LC-LC MM 1m OM4"
* 6ks Optický patch kabel duplex LC-LC MM 5m OM4"
* 2ks Optický patch kabel duplex LC-LC SM 15m OS2"
* 9ks 10G SFP+ to SFP+ 1m Direct Attach Copper Cable
* 6ks 10G SFP+ to SFP+ 3m Direct Attach Copper Cable
* 1ks Stack 50Gb QSFP56 to SFP56 0.65m DAC Cable pro Core switche
* Kabely a transceivery musí být od totožného výrobce jako poptávané Core switche z důvodu zajištění kompatibility
1. **Zálohovací software – suma**
* Licence pro zálohování 20ks serverů (virtuálních, nebo fyzických, nebo kombinace obou) s podporou na 36 měsíců
* Podpora páskové dvoumechanikové knihovny s minimálně 24 sloty a mechanikami minimálně LTO-9
* Podpora níže specifikované páskové knihovny
* Zálohovací řešení musí podporovat infrastrukturu VMware ve verzích 6.x, 7.x a 8.0, včetně VMware Cloud Foundation, VMware Cloud on AWS, VMware cloud on Dell a Azure VMware Solution
* Řešení musí podporovat hostitele spravované serverem VMware vCenter ve verzích 6.x, 7.x a 8.0 i samostatné ESXi hostitele.
* Zálohovací řešení musí podporovat Windows Server Hyper-V 2012 až 2022 včetně Server Core, Azure Stack HCI i Microsoft Hyper-V Server
* Řešení musí podporovat hostitele spravované pomocí Microsoft System Center Virtual Machine Manager 2012 R2 až 2019, klastrové i samostatné hostitele Hyper-V
* Řešení musí podporovat zálohování všech operačních systémů, které jsou podporovány pro provoz na těchto hypervizorech
* Řešení musí podporovat zálohování platformy Red Hat Virtualization 4.4 SP1
* Řešení musí podporovat zálohování celých zařízení NAS, jednotlivých sdílených složek SMB a NFS a souborových serverů Windows a Linux.
* Software musí být možné licencovat pomocí trvalé licence i formou časově omezené subscripce.
* Řešení nesmí být závislé na jednom poskytovateli HW, virtualizační, nebo cloudové platformy a to jak pro výpočetní část, tak pro část ukládání dat.
* Licence musí být přenositelná mezi různými fyzickými, virtuálními a cloudovými chráněnými objekty
* Všechny součásti řešení musí plně podporovat komunikaci po IPv6
* Řešení musí mít mechanismy k úspoře objemu úložného prostoru pro ukládání záloh. Jejich využití musí být volitelné a nesmí omezit žádné funkcionality zálohování a obnovy dat.
* Řešení musí poskytovat jednotnou konzoli pro přehled o zálohách fyzických, virtuálních, cloudových, NAS i Kubernetes prostředí
* Řešení musí umožnit vytvoření jednoho logického úložiště pro ukládání záloh z neomezeného počtu různorodých diskových úložišť
* Řešení musí umožňovat ukládání záloh do různých diskových úložišť, souborových systémů, objektových úložišť, nebo deduplikačních diskových zařízení.
* Řešení musí využívat mechanismus sledování změn bloku. Pro všechny podporované hypervizory musí být implementace CBT certifikována výrobcem hypervizoru
* Výše uvedená funkce musí být konfigurovatelná na úrovni datastore virtualizační platformy
* Řešení musí umožňovat vytváření záloh integrací se snímky úložiště. Dále musí umožnit obnovu jednotlivých VM, souborů a položek aplikace z těchto snímků. Proces zálohy nemůže k připojení snímku použít dočasného hostitele. Popsaná funkce musí fungovat pro prostředí VMware vSphere a musí podporovat následující pole: Dell, NetApp, HPE, HITACHI VANTARA, IBM, Lenovo, Fujitsu, Pure Storage, CISCO, DataCore
* Řešení musí mít replikaci produkčních VM přímo z infrastruktury VMware vSphere, mezi hostiteli ESXi, včetně asynchronní nepřetržité replikace. Řešení musí navíc umožnit jako zdroj replikačních úloh využít soubory záloh
* Řešení musí umožňovat okamžitou obnovu více virtuálních strojů současně, přímo ze záložních souborů z libovolného bodu obnovení (vestavěný NFS server). Tato funkce musí být podporována pro prostředí VMware a Hyper-V a musí fungovat bez ohledu na hardware používaný k ukládání záložních souborů VM
* Uvedená funkce musí umožňovat spuštění zálohy vytvořené z různých platforem (různých virtuálních, fyzických a veřejných cloudových virtuálních strojů)
* Řešení musí umožňovat online migraci virtuálních počítačů, zpuštěných z úložiště záloh, do produkčního úložiště pomocí funkcí hypervizoru. Řešení musí také poskytovat svou vlastní funkci, která takové schopnosti poskytne.
* Řešení musí umožňovat prezentaci disků přímo ze záložního souboru do spuštěné VMware VM
* Přístup do řídící konzole musí být chráněný vícefaktorovou autentizací bez nutnosti přístupu k internetu.
* Řešení musí umožňovat vytváření záloh odolných vůči náhodnému, či úmyslnému smazání, nebo ransomware útokům na komoditním serverovém HW, nebo jakémkoliv S3-kompatibilním objektovém úložišti
* Řešení musí podporovat gMSA účty pro zajištění aplikačně-konzistentních záloh v GuestOS bez nutnosti ukládání přístupových oprávnění na úrovni administrátora pro daný GuestOS.
* Řešení nesmí použít centrální databázi pro ukládání jakýchkoli metadat deduplikace. Ztráta databáze nemůže způsobit, že záložní soubory budou nestabilní. Metadata deduplikace musí být uložena v záložních souborech
* Řešení musí umožňovat pravidelné automatické testování obnovitelnosti záloh, včetně funkčnosi jednotlivých služeb a kontrolou obsahu na kybernetické hrozby pomocí řešení třetích stran.
* Řešení musí poskytovat dohled nad chráněnou virtualizační platformou, poskytující včasná varování před výpadkem, nebo omezením dostupnosti produkčního prostředí
* Řešení musí poskytovat možnost dohledu služeb a procesů provozovaných v GuestOS jednotlivých chráněných VM
* Řešení musí informovat, které VM nejsou chráněné dostatečně, nebo vůbec a zároveň kdy a jakým způsobem byl naposledy vytvořen bod obnovy.
* Řešení musí poskytovat možnost automatizovaných řešení chybových stavů
* Řešení musí poskytovat funkce pro zasílání stavových hlášení do centrálního monitorovacího nástroje přes SNMP protokol
* Řešení musí podporovat monitorování virtualizovaných prostředí VMware vSphere a Microsoft Hyper-V bez nástrojů třetích stran
* Řešení musí podporovat dohled následujících systémů: VMware, ESXi 6.x, 7.x a 8.0 pro placené i bezplatné edice ESXi. Podporovaní hostitelé mohou být spravováni pomocí vCenter serveru nebo pracovat v samostatném režimu
* Řešení musí poskytovat historická data a predikce z nich vyplývající, nezbytné pro plánování zdrojů pro provoz a ochranu virtualizovaného prostředí
* Součástí řešení musí být i možnost vytvářet detailní auditové správy o změnách v konfiguraci zálohovacího řešení a o obnovách dat ze záloh
* Řešení musí podporovat reporting virtualizovaných prostředí VMware vSphere a Microsoft Hyper-V bez nástrojů třetích stran
* Řešení musí podporovat reporting následujících hypervisorových systémů: VMware, ESXi 6.x, 7.x a 8.0 pro placené i bezplatné edice ESXi. Podporovaní hostitelé mohou být spravováni vCenter nebo pracovat v samostatném režimu
* Řešení musí podporovat reporting následujících systémů: Microsoft Server Hyper-V 2012, 2012R2, 2016, 2019 a 2022 pro placené i bezplatné edice. Podporovaní hostitelé mohou být spravováni SCVMM nebo pracovat v samostatném režimu
* Řešení nesmí vyžadovat instalaci žádných agentů na monitorovaných hostitelích ESXi a Hyper-V a na virtuálních počítačích
1. **NAS zařízení – 1 ks**
* Rack provedení výšky 2U
* 12x šachta na za chodu vyměnitelný pevný disk
* Možnost osadit disky 3,5“ SATA, 2,5“ SATA a 2,5“ SSD
* Výměna disků za provozu
* Možnost rozšíření o další diskovou polici
* Podpora RAID 0, 1, 5, 6 a 10
* 1x CPU 4 CORE
* 8 GB RAM, 1x volný RAM slot, možnost rozšíření až na 32 GB RAM
* 1x RJ-45 10GbE LAN port
* 2x RJ-45 1GbE LAN port (s podporou funkcí Link Aggregation / Failover)
* 2x USB 3.2
* 1x eSATA port
* 1x PCIe slot x8 Gen3
* 2x redundantní napájecí zdroj
* Sada lyžin pro montáž do racku
* Podpora virtualizace VMware ESXi 6.5 and VAAI, Windows Server 2022, Citrix Ready, OpenStack
* Podporované protokoly: SMB1 (CIFS), SMB2, SMB3, NFSv3, NFSv4, NFSv4.1, NFS Kerberized sessions, iSCSI, HTTP, HTTPs, FTP, SNMP, LDAP, CalDAV
* Osazeno 8x diskem 20TB 3,5“ SATA 7k2 rpm, 6GB/s, 256 MB cache
* Včetně kompletní instalace a konfigurace
* Záruka 36 měsíců
1. **Vícefaktorové ověřování - soubor**

**200ks token - hardwarový klíč velikosti klíčenky**

* Integrovaná baterie s výdrží min. 2 roky
* Displej s ukazatelem OTP kódu, časového limitu a stavu baterie
* Centrálni management z FortiGate nebo FortiAuthenticator
* Bez nutnosti instalace klientského softwaru
* Časový interval OTP kódu min. 30s
* Stupeň krytí min. IP65
* Podpora standardu OATH/TOTP a HMAC-SHA1
* 100% kompaktibilní s níže popsanou 2FA appliancí – totožný výrobce

**Softwarový token – aplikace pro 25 uživatelů**

* Podpora platforem iOS a Android
* Podpora Apple Watch
* Přenos tokenů napříč platformami
* Aplikace chráněná kódem PIN/otiskem prstu
* Zobrazení časového intervalu OTP
* Zobrazení sériového čísla tokenu
* Ochrana aplikace proti hrubému vymazání ze zařízeni
* Potvrzení přihlášení jednim klepnutím
* Aplikace nemá přístup do uložiste telefonu
* Aplikace nemá přístup do uložiště zařízeni (nemůže měnit nastavení, nahrávat zvuk, číst emaily a kontakty)
* Centrálni management z FortiGate nebo FortiAuthenticator
* Nemožnost vzdáleného vymazáni zařízeni ani přes management konzolu
* Generování OTP kódů v offline režimu (zařízení není připojeno k internetu)
* 100% kompaktibilní s níže popsanou 2FA appliancí – totožný výrobce

**Virtuální 2FA appliance pro platformu VMWare, Hyper-V, KVM**

* Management identit, plnohodnotná AAA funkcionalita, integrované funkce AAA pro připojení z VPN
* Podpora nabízených funkcí pro minimálně 300 uživatelů
* Možnost automaticky synchronizovat uživatele z Active Directory
* Možnost vytvářet lokální uživatele a skupiny
* Podpora 2FA pomocí tokenů (aplikace pro iOS a Android, HW token)
* Podpora 2FA pomocí SMS a emailu
* Podpora ověřováni ze sociálních sítí (Facebook, LinkedIn)
* Možnost definovat zařízení na základě MAC adresy
* Funkce LDAP/LDAPS serveru
* Možnost automatického importu identit ze vzdálených LDAP serverů
* Funkce TACACS+ serveru
* Funkce Radius serveru
* Podpora radius accountning v proxy režimu
* Funkce SAML IdP
* Možnost napojení a ověřování z externího Radius, LDAP SAML a OAuth server
* Podpora SSO autentizace uživatelů v prostředí domény MS Windows
* Podpora Kerberos
* podpora EAP metod EAP-MSCHAPv2, EAP-TLS, PEAP, EAP-GTC
* Funkce certifikační autority
* Podpora SCEP a CRL
* Podpora captive portálu
* Podpora samoobslužných portálů (reset hesla, editace uživatelských údajů, přidělení tokenů)
* Podpora 2FA pro Outlook Web Access pomocí nativního klienta
* Podpora mechanismu 2FA pro koncové stanice a přihlášení do systému Windows
* Podpora push notifikací pro 2FA a mobilní aplikaci
* Podpora REST API (pokud tato funkce vyžaduje licenci, tak musí být součástí dodávky)
* Podpora minimálně 3 roky
1. **Firewall (NGFW) – 1 ks**

**Základní technické požadavky**

* HW appliance o velikosti 1 RU s možností rozšíření o druhý box do režimu vysoké dostupnosti (active-active, active-passive)
* grafické konfigurační rozhraní a příkazový řádek
* min. 12 metalických RJ-45 portů 10/100/1000
* min. 4 optická datová rozhraní SFP+ o rychlosti 10Gb/s
* min. 4 optická datová rozhraní SFP o rychlosti 1Gb/s
* 1 dedikovaný port pro správu pomocí konzole pro přístup k CLI a 1 management port
* NGFW musí podporovat plnohodnotnou inspekci sítového provozu v režimech:
* NAT/router
* L2 transparentní režim (dva a více sítových rozhraní)
* L2 interface pair (dvě sítové rozhraní)
* Redudantní napájení firewallu

**Výkonové požadavky**

* Minimální požadovaná propustnost stavového firewallu pro IPv4 i IPv6 provoz 35 Gbps (UDP pakety o velikosti 512 B)
* Nízké vložené zpoždění zařízení (latence) max. 5ěs
* Minimální počet současně navázaných spojení firewallu 2.5 M
* Minimální počet nových spojení za sekundu 120 k
* Propustnost firewallu v packetech min. 40 Mpps
* Propustnost NGFW (kombinace stavového firewall, IPS, rozpoznávání aplikací na L7, logování) minimálně 3 Gbps
* Propustnost ochrany proti hrozbám a škodlivému kódu (kombinace stavového firewall, IPS, rozpoznávání aplikací na L7, ochrana proti škodlivému kódu, logování) min. 2.5 Gbps
* Propustnost ochrany proti hrozbám (IPS, ochrana proti sítovým útokům, logování) min. 5 Gbps
* Propustnost funkce rozpoznávání sítových aplikací na L7 min. 5 Gbps
* Propustnost IPSEC VPN v konfiguraci AES256/SHA256 min. 30 Gbps
* Propustnost funkce SSL inspekce provozu min. 2.7 Gbps
* Min. počet konfigurovatelných virtuálních kontextů na každém zařízení = 10

**Funkční požadavky**

* Funkce rozpoznávání kancelářských aplikací na L7 – aplikační vrstvě, podpora alespoň 3000 kancelářských aplikací, protokolů či příkazů; jednotlivé aplikace/protokoly uspořádány do kategorií; výrobce automaticky udržuje a aktualizuje databázi podporovaných aplikací
* Funkce ochrany před sítovými útoky vycházející z výrobcem udržované a aktualizované databáze, ochrana před útoky typu DoS, verifikace protokolů, min. 10 000 signatur v databázi; podpora zabezpečení kancelářských (IT)
* Ochrana před výskytem škodlivého kódu v síťovém provozu (antivirus/antimalware) s podporou zabezpečení kancelářských (IT) a škodlivého kódu pro mobilní zařízení; podpora funkce sanitarizace dokumentů (odstranění aktivního obsahu) a předání zkoumaných souborů pro analýzu v prostředí typu sandbox
* funkce kategorizace webových stránek (web filtering) s podporou minimálně 60 kategorií (pracovní zájmy, osobní zájmy, stránky se škodlivým kódem, nově registrované domény atp.), podpora definice časové kvóty, kterou nesmí daný uživatel na dané kategorii za den překročit, výrobcem aktualizovaná a udržovaná databáze
* funkce SSL inspekce pro kontrolu protokolů s možností vytváření výjimek
* Výjimka z SSL inspekce na základě administrátorem definovaných adres
* Výjimka z SSL inspekce na základě kategorie URL, brané z URL filtrační databáze (např. kategorie bankovnictví, zdravotnictví atd.)
* Ověřování identity uživatelů (možnost napojení na MS Active Directory, LDAP, Radius, Kerberos), práce s identitou uživatele v bezpečnostní politice firewallu v režimu tzv. Single Sign-On
* Funkce dynamického routingu (min. BGP, OSPF, RIP), pokud jsou tyto funkce licencované, tak licence musí být součástí dodávky
* Funkce QoS, traffic shaping
* Funkce klientské VPN (přístup do VPN v tunelovém režimu s VPN klientem a přístup do VPN přes webový portál, možnost aplikace identit uživatele ve smyslu definice bezpečnostní politiky VPN uživatelů
* Site-to-Site IPsec VPN s podporou statického i dynamického routování
* Podpora výrobce v režimu 24x7 a aktualizace všech požadovaných bezpečnostních funkcí po dobu 3 let
* Umístění výrobce v Gartner MQ for Network Firewalls v sekci „Leaders“ v posledních min. 3 letech
* 2x 10Gb SFP+ modul FC konektor multimode pro firewall
1. **Záložní pásková knihovna – 1 ks**
* Knihovna musí obsahovat minimálně 24 slotů
* 2x FC drive minimálně LTO-8
* Instalace do racku, velikost max 2U
* Planá kapacita knihovny 288TB bez komprese, 720TB s kompresí
* Možnost mixovat LTO mechaniky různých generací
* Možnost mixovat LTO pásky různých generací
* 30ks minimálně LTO-8 RW medií včetně čárových kódů
* 1ks čistící LTO pásky
* 1ks single port FC PCI-E adapter 16Gb pro server, který zadavatel již vlastní
* FC kabel LC/LC OM4 MM 3m mezi server a knihovnu
* Záruka 3 roky garantovaná výrobcem. Doba servisního zásahu na místě u zákazníka musí být garantována výrobcem knihovny. Délka záruky musí být ověřitelná na webu výrobce dle sériového čísla knihovny.
* Zařízení musí být nové, nepoužité s garancí výrobce a určené přímo pro český trh.
* Pro centrální management požadujeme páskovou knihovnu od totožného výrobce jako diskové pole a servery, které zadavatel používá, tak aby byla využita synergie jednotné správy takového prostředí
* Součástí dodávky musí být kompletní instalace knihovny, včetně konfigurace a nastavení zálohovacích úloh dle požadavků zadavatele.
1. **Monitoring infrastruktury – 1 ks**

Základní vlastnosti monitorovacího systému

* Produkt je open source – trvalá licence
* Výrobce vytváří verze s Long-term support (LTS)
* Výrobce nabízí možnost placené podpory
* Data lze uchovávat minimálně 1 rok
* Data se po určitém čase začnou průměrovat pro snížení velikosti databáze
* Systém podporuje proxy servery pro monitoring vzdálených lokalit, provoz ze vzdálených lokalit je šifrovaný
* Se systémem je možné pracovat přes API
* Podporované metody vyčítání dat
* ICMP
* SNMP
* SNMP trap
* IPMI
* JMX
* Agent pro Windows, Linux, macOS, FreeBSD
* Web monitoring
* podpora monitoringu pomocí vlastních skriptů
* Šablony sledovaných zařízení
* Výrobce musí mít připravené šablony pro:
* Fortigate firewall
* HP Switche
* Aruba Switche
* Cisco Switche
* VMware Hypervizor
* HyperV Hypervizor
* HP ILO
* Synology NAS
* APC UPS
* Windows server
* Linux server
* MS Exchnage
* Možnost vytvářet vlastní šablony
* Možnost importu šablon vytvořených komunitou
* Možnost použití maker v šablonách, každé zařízení může mít nastavenou jinou hranici pro spuštění alertu

Sledování hodnot

* Možnost změny monitorovacího intervalu (vteřiny, hodiny, dny) = optimalizace velikosti DB
* Možnost změny délky ukládání dle typu hodnoty (text, číslo) = optimalizace velikosti DB
* Možnost přepočítání sledované hodnoty před uložením do DB (např. násobení) = změna jednotky (bit/Byte apod.)
* Možnost vytvoření vlastní hodnoty, která se vypočítá z jiných nasbíraných hodnot (např. Total Bytes - Free bytes = Used bytes)
* Možnost mapování sledovaných hodnot na textové výrazy (1=on, 2=off, 0=unknown)
* Notifikace
* Možnost posílat notifikace na:
* e-mail
* SMS
* MS Team
* Discord
* Telegram
* Možnost definovat vlastní strukturu textu notifikací
* Možnost posílat notifikace při problému a po vyřešení
* Možnost posílat notifikace jen pro vážnější alerty
* Možnost eskalace notifikací (pokud není opraveno do 1h, notifikace se odešle znovu a přidají se další adresáti)
* Možnost provozovat TV/monitor s dashboadem se zvukovými notifikacemi
* Možnost vytvoření návazností mezi alerty (v případě výpadku switche nebude systém hlásit nedostupnost zařízení do něj připojených)

Uživatelské rozhraní

* Možnost vytvářet skupiny uživatelů s různými oprávněními k různým zařízením
* Možnost napojení rozhraní na LDAP a SAML
* Jazyk rozhraní je v češtině, slovenštině a angličtině
* Každý uživatel si může vytvořit vlastní dashboard a zvolit vlastní jazyk rozhraní
* Rozhraní umožní uživatelům komentovat alerty, např. informovat, že na odstranění problému se už pracuje
* Rozhraní umožní volbu vlastního časového intervalu pro zobrazení hodnot v grafu
* Rozhraní umožní zobrazení více sledovaných hodnot v jednom grafu (možnost korelovat data)
* V grafech musí být pro lepší orientaci zvýrazněna pracovní a mimopracovní doba

Další požadavky

* Systém musí umožňovat automatické skenování sítě, nově objevená zařízení budou automaticky přidána ke sledování nebo bude správci odeslán e-mail s upozorněním na nové zařízení v sítí
* Systém musí umožnovat výpočet SLA pro jednotlivé sledované služby s možnosti vygenerování měsíčního/ročního reportu
* Systém musí umožňovat automatické vytváření inventáře zařízení ze sledovaných hodnot (Jméno, SN, MAC, OS apod.)
* Systém musí umožňovat uvedení skupiny zařízení do módu údržby a předejít tak posílání notifikací při údržbě zařízení
* Systém musí umožňovat vytváření vlastních „map“, kde mapy mohou ukazovat umístění porouchaného zařízení v rámci půdorysu budovy nebo v rámci racku v serverovně
* Systém musí umožňovat nahlížení do historie problému i několik měsíců zpětně
* Dodavatel provede zaškolení 2 pracovníků zadavatele v rozsahu 8 hodin na obsluhu a nastavení systému.

1. **LOG Management – 1 ks**
* HW appliance (montáž do běžného 19‘‘ datového rozvaděče, výška max. 1U) pro zpracování událostí z předdefinovaných zdrojů logů napříč výrobci aplikací, operačních systémů a síťového hardware.
* Redundantní zdroje a ventilátory. Ventilátory za provozu vyměnitelné.
* 1x CPU min. 16 jader s podporou HyperThreadingu nebo Multi-Threadingu.
* Operační paměť RAM 64GB DDR-4.
* 4x 1GbE RJ45 síťové rozhraní včetně link agregace dle LACP (802.3ad), VLAN a IP adresace v jednotném webovém rozhraní systému.
* Průměrný trvalý příjem událostí/s. (průměrná délka zprávy min. 700Byte) 2000 událostí/s.
* Špičkový příjem bez ztráty dat po dobu nejméně 10 minut (průměrná délka zprávy min. 700 Byte) 4000 událostí/s.
* Čistá velikost integrované databáze 12 TB.
* Jedna webová console pro všechny administrátorské i operátorské činnosti.
* Licenčně neomezený počet zařízení pro příjem zasílaných událostí. Licenčně neomezený počet událostí v GB za den nebo licence na minimálně 200GB uložených událostí za den.
* Příjem a zpracování logů, události a další strojově generovaná data prostřednictvím protokolů SYSLOG (RFC3164, RFC5424, RFC5425), RELP.
* Bezagentový sběr událostí, vyjma podpory sběru na pobočkách a agenta pro sběr Windows logů.
* Windows agent musí současně podporovat jak monitoring interních windows logů, tak monitoring textových souborových logů.
* Windows agent se nesmí instalovat individuálně, ale prostřednictvím MS AD Group Policy a nesmí vyžadovat žádnou konfiguraci na cílovém systému, tzn., že musí být centrálně spravovaný a jeho konfigurace musí být kompletně realizována v grafickém rozhraní systému bez využití skriptů nebo maker.
* Windows agent musí podporovat centralizovanou konfiguraci Microsoft Sysmon pro obohacení logů, včetně globálního a selektivního zapínaní/vypínaní služby Sysmon a výběr z několika přednastavených konfigurací Sysmon v grafickém rozhraní centrální správcovské konzole systému.
* Komunikace Windows agenta a centrálního systému musí být zabezpečena TLS 1.2 a výše a musí podporovat ověřování certifikátem.
* Windows agent musí podporovat sběr nejen ze základních systémových logů (Aplikace, Zabezpečení, Instalace, Systém), ale i sběr všech ostatních logů ve složce Protokoly aplikací a služeb a logy rozšířené Sysmonem.
* Windows agent musí ke všem odesílaným událostem automaticky doplňovat jejich textový popis tak, jak je zobrazen v Prohlížeči událostí (Event Viewer) na koncovém systému. K významným bezpečnostním událostem musí doplňovat značku a popis dle MITRE ATT&CK matrice a k takto detekovaným procesům a souborům automaticky vytvářet SHA256 hash.
* Počet instalací Windows agenta nesmí být licenčně a časově omezen. Pokud je Windows agent licenčně nebo časově omezen, požadujeme dodání licencí na Windows agenty v množství 450 na dobu předpokládané morální životnosti produktu – 7 let.
* Výrobcem vytvářené parsery pro běžné systémy.
* Uživatelsky definované parsery - systém umožňuje dopsání parserů pro další zdroje log zařízení uživatelem pomocí tzv. vizuální programování, bez nutnosti spolupráce s výrobcem.
* Standardizace přijatých logů do jednotného formátu a jejich normalizace (rozdělení) do příslušných polí dle jejich typu. Vytvoření vlastního důvěryhodného časového razítka ke každému logu.
* Uchování originální verze přijatých logů/zpráv včetně původní časové značky události.
* Okamžitá a automatická indexace umožňující okamžité prohledávání událostí.
* Podporované formáty RAW, Syslog (RFC5424), CEF, LEEF, JSON (RFC8259).
* Systém nesmí umožnit mazání nebo modifikování již uložených logů v rámci požadované retence. (ani libovolnou konfigurační změnou)
* Automatické doplňování reverzních DNS záznamů, čísel a jmen ASN systému a geolokace ke všem přijatým událostem a všem polím, obsahujícím IP adresy.
* Nativní získávání logů z Office365 prostředí s licencí E3 bez nutnosti instalovat dodatečné externí komponenty.
* Ověřování uživatele na externím LDAP serveru resp. ověření lokálního účtu v případě výpadku LDAP.
* Grafické rozhraní musí umožňovat filtraci nerelevantních událostí, snadné vyhledávání událostí, vytváření reportů a dynamickou vizualizaci událostí.
* Reportovací nástroj s přednastavenými nejběžnějšími reporty a možností vlastních úprav a vytvoření nových pohledů.
* Uložení uživatelem vytvořených pohledů na data (dashboardů) pro budoucí zpracování.
* Podpora základní funkce SIEM - funkce pro korelace událostí a upozornění s hraničními limity.
* Výrobcem předpřipravené sety/vzory alertů a korelací.
* Monitoring stavu systému - alertování při překročení prahových hodnot SMTP nebo Syslog.
* REST-API pro integraci s externím monitorovacím systémem (např. Zabbix, Nagios, MRTG).
* Systém pro vzdálenou správu serveru včetně potřebné licence, pokud je třeba.
* Dedikované síťové rozhraní pro management HW 1x 1GE RJ45.
* Uživatelské role definující přístupová práva k uloženým událostem a jednotlivým ovládacím komponentům systému.
* Aktualizace systému přes centrální webovou správcovskou konzoli v jednom balíku.
* Podpora zálohování nebo obnovení konfigurace v jednom kroku a jednom souboru pro celý systém.
* Podpora komprese ukládaných dat.
* Podpora důvěryhodného zálohování komprimovaných dat na externí systém.
* Servisní podpora na HW s opravou v místě instalace serveru, s garantovanou NBD od nahlášení závady 36 měsíců.
* Servisní podpora na SW v rozsahu aktualizaci systému a parserů, opravy chyb a telefonickou a emailovou podporu s diagnostikou vzdáleným přístupem 60 měsíců.

**Požadavky na implementaci**

* Montáž do racku.
* Připojení do LAN infrastruktury.
* Aktualizace FW a OS.
* Napojení a sběr všech významných log zdrojů stávající a pořizované infrastruktury zadavatele – (firewally, LAN prvky, servery, OS, aplikace atd.).
* Nastavení reportingu.
* Nastavení alertů.

**Ověření kontroly funkčnosti systému**

* Základní nastavení systému a jeho konfigurace tak, aby mohl pracovat v prostředí zadavatele, včetně vytvoření uživatelů s rozdílným systémovým i databázovým oprávněním, a to v jednotném webovém rozhraní nabízeného systému.
* Zapojení pěti vybraných zdrojových systémů logů odesílajících logy prostřednictvím Syslog protokolu přes UDP/TCP/TLS z prostředí zadavatele a otestování následujících vlastností:
* nastavení klasifikace zdrojů;
* nastavení značek (tagů) pro vybrané zdrojové systémy;
* filtrování událostí;
* úprava normalizace existujícího zdroje v grafickém rozhraní nástroje;
* vytvoření reportů a exportu logů a vybraných údajů z logů.
	+ Konfigurace pěti vybraných systémů Microsoft Windows tak, aby posílaly EVTx a textové logy do testovaného systému, s konfigurací pouze v jednotném grafickém rozhraní nabízeného systému.
	+ Ověření funkčních a výkonových parametrů Windows agenta a jeho centralizované správy v nabízeném systému včetně centrální instalace a centrální konfigurace Microsoft Sysmon služby pro rozšíření hodnoty logů vytvářených zdrojovými systémy dle doporučené auditní politiky.
	+ Konfigurace kolektoru logů z jedné databáze z prostředí zadavatele v jednotném webovém rozhraní nabízeného systému bez nutnosti instalovat na databázový server další produkty třetích stran.
	+ Oprava ze záloh po simulovaném úplném selhání nabízeného systému v následujících krocích:
* provedení zálohy konfigurace a dat na externí systém;
* vytažení dvou libovolných disků za běhu systému;
* nastavení systému do továrního nastavení;
* obnovení konfigurace a všech dat z vytvořených záloh;
* kontrola úplnosti obnovené konfigurace a dat ze záloh.
	+ Navýšení a ponížení software nabízeného systému v grafickém rozhraní a provedení kontroly, že v případě ponížení nedojde ke ztrátě dříve shromážděných dat.
	+ Kontrola, jakým způsobem se nastavuje systém ve vysoké dostupnosti (vytvoření clusteru) v jednotném webovém rozhraní systému a úplnost dokumentace k možným havarijním scénářům.
	+ Kontrola výkonu systému v běžné zátěži – generátorem logů se odešle vzorek originálních dat sesbíraných během předchozích testů. A to rychlostí odpovídající nabízenému systému po dobu minimálně 30 minut. Sledované hodnoty budou: přijetí všech logů a jejich správné zařazení do databáze s časovým razítkem odpovídajícím skutečné době přijetí logu. Dále bude provedena kontrola, zda nedošlo během zpracování logů k jejich poškození nebo ztrátě. Logy musejí být kompletně zpracovány bez ztráty dat, se správným časovým razítkem uloženy v databázi, normalizovány a doplněny o rozšiřující informace typu metadata, DNS-PTR a geolokace.
	+ Kontrola výkonu systému v krátkodobém přetížení – generátorem logů se odešle vzorek originálních dat sesbíraných během předchozích testů. A to rychlostí odpovídající dvounásobku výkonu nabízeného systému po dobu 10 minut. Sledované hodnoty budou: přijetí všech logů a jejich správné zařazení do databáze s časovým razítkem odpovídajícím době přijetí logu systémem. Dále kontrola, zda nedošlo během zpracování logů k jejich poškození nebo ztrátě. Logy musejí být kompletně zpracovány bez ztráty dat, se správným časovým razítkem uloženy v databázi, normalizovány a doplněny o rozšiřující informace typu metadata, DNS-PTR, číslo a jméno ASN a geolokace.
* Součástí ověření funkčních vlastností může být i ověření požadované funkcionality a parametrů dodaného systému dle Technické specifikace tohoto zadání.
* Ověření funkčních vlastností nabízeného systému bude provádět zadavatel, vycházeje z dokumentace k nabízenému systému. V případě nejasností zadavatel vyzve k účasti zástupce dodavatele, který mu poskytne potřebnou součinnost, a to maximálně do 3 pracovních dnů po doručení výzvy dodavateli. Testy budou provedeny v prostředí zadavatele.
1. **Instalace a implementace – soubor**
* Rozbalení veškerého dodaného HW, kontrola bezvadného stavu, likvidace přepravního a obalového materiálu a spolupráce s dodavatelem na evidenci HW (případné opatření evidenčními štítky);
* Instalace a zprovoznění veškerého dodaného HW do stávajících 19“ rozvaděčů a provedení funkčních testů;
* Instalace a zprovoznění veškerého dodaného SW na nově dodaný (i stávající) HW;
* Implementace zálohovacího SW v souladu s metodikou výrobce na odolnost diskových úložišť záloh před útoky ransomware;
* Nastavení LAN komponent tak, aby odpovídalo po konceptuální stránce stávajícímu schématu, tedy byly schopny rozšířit, popř. převzít funkci původní infrastruktury, tj. tak, aby nastavení firewallu odpovídalo aktuálnímu stavu a switche byly zapojeny v patřičné topologii tak, aby umožňovaly serverům komunikaci nutnou k následující fázi konfigurace a zprovoznění nového produkčního prostředí;
* Zavedení veškerého dodaného HW do monitoringu dodavatele i objednatele;
* Instalace veškerého dodaného SW a jeho zavedení do monitoringu objednatele;
* Nastavení monitoringu zálohování na úroveň jednotlivých HW a SW složek zálohovacího řešení, zálohovacích úloh a jejich průběhu;
* Úprava konfigurace datového centra tak, aby stávající produkční prostředí a služby jím poskytované byly provozovány, monitorovány, zálohovány a zabezpečeny na nově dodaném HW a SW;
* Plné zanesení virtualizace do monitoringu objednatele;
* Provedení testu výkonu spojení mezi jednotlivými komponentami a disaster recovery při zátěži pro vyloučení SPOF;
* Integrace zálohování s virtualizační konzolí;
* Požadujeme instalaci základního zálohovacího SW (řízení, správa)
* Požadujeme instalaci všech potřebných serverů pro transport dat (data moover, media server, proxy server)
* Pokud má backup SW oddělené GUI klienty pro správu, požadujeme ukázkovou instalaci takové admin konzole na OS Linux
* Pokud má backup SW oddělené zálohovací klienty pro zálohování daných OS, požadujeme ukázkovou instalaci na vybraných OS (Windows, Linux)
* Požadujeme backup SW integraci s administračními nástroji pro virtualizované prostředí MS Windows a VMware
* Požadujeme zviditelnění a nakonfigurování všech uvažovaných cílů záloh (VTL zařízení, D2D zařízení)
* Požadujeme konfiguraci všech rozhraní (LAN/SAN) na všech serverech sloužících pro transport zálohovaných dat (data moover, proxy servery, media servery, storage servery) s optimalizací na:
* HA (vysokou dostupnost),
* propustnost (agregace více linek)
* Na všech komponentách zálohovacího eko-systému implementovat administraci a přístupy s ohledem na RBAC (Role Based Access Control) včetně napojení na centrální AD/LDAP.
* Požadujeme vytvoření automatizovaného reportovacího systému, který bude informovat o nedokončených zálohovacích úlohách
* požadujeme ukázku monitoringu:
* stavy-statusy jednotlivých komponent (řídící serever, data moover, cíl záloh)
* stavy-statusy úloh, statistiky úloh
* kapacity, využité a volné kapacity v jednotlivých cílech záloh
* Požadujeme dodání elektronické dokumentace (pdf) ke všem použitým SW komponentám (user guide, admin guide, config guide atp.)
* Požadujeme vytvoření a předání dokumentace o konkrétním provedení a nastavení celého zálohovacího prostředí. (otevřený editovatelný formát ODF např. \*.odt nebo MS Office formát např. \*.docx)
* Zanesení dokumentace prostředí do Redmine objednatele popř. předání formou dokumentů ve formátech odt, docx či pdf;
* Zadavatel požaduje kompletní instalaci bezpečnostního software na všechna zařízení v jeho vlastnictví, včetně mobilních zařízení (tablety, mobilní telefony)
* Dokumentace jednotlivých HW a SW komponent musí mít část věnující se instalaci, konfiguraci, běžné administraci a užívání.
1. **Zaškolení obsluhy – soubor**
* Zaškolení 2 zaměstnanců zadavatele v obsluze a údržbě zařízení v rozsahu 16 pracovních hodin na dodaném zařízení v místě plnění (s min rozsahem 8 pracovních hodin na zařízení LOG management).

**V následující tabulce účastník zadávacího řízení vyplní, zda a jakým způsobem splnil požadavky zadavatele:**

1. Zadavatel požaduje, aby dodavatelem nabízené HW zařízení, případně SW aplikace, splňovaly **veškeré** výše uvedené minimální požadavky (funkcionality a parametry) a tyto byly zahrnuty v jeho nabídce a v celkové ceně.
2. Dodavatel **jednoznačně deklaruje** splnění, popřípadě absenci každého minimálního požadavku ve výše uvedených tabulkách, a to vyplněním příslušného pole „Splněno“ jednou ze dvou nabízených možností:
* **ANO** - v případě, že dodavatelem nabízené plnění minimální požadavek splňuje,

nebo

* **NE** - v případě, že dodavatelem nabízené plnění minimální požadavek nesplňuje.

Tabulky s vyplněním polí „Splněno“ budou nedílnou součástí nabídky. V případě **nevyplnění** požadovaných údajů zadavatel **vyloučí** dodavatele z účasti v zadávacím řízení.

1. V případě, že dodavatel v příslušné položce pole neoznačí nebo v položce budou označeny obě možnosti dle bodu 2., bude taková položka posuzována jako neoznačená a bude znamenat vyloučení dodavatele z důvodu nesplnění zadavatelem požadovaného minimálního plnění.
2. V případě, že dodavatel v příslušné položce pole označí **NE**, bude taková položka posuzována jako nesplnění minimálních požadavků zadavatele a bude znamenat vyloučení dodavatele z důvodu nesplnění zadavatelem požadovaného minimálního plnění.
3. Dodavatel do sloupce „Popis řešení“ uvede, zda jím dodané HW zařízení, případně SW aplikace, splňuje jednotlivé požadavky zadavatele a **výstižně** (minimálně uvedením názvu výrobce a obchodního či typového označení nabízeného řešení) doplní, jakým způsobem je požadovaná funkčnost splněna.

| **Č.** | **Kritérium** | **Splněno** | **Popis řešení** |
| --- | --- | --- | --- |
| 1. | UPS záložní zdroj | ANO / NE | …………………….……… |
| 2. | Síťová infrastruktura – core switch (vč. příslušenství) | ANO / NE | …………………….……… |
| 3. | Zálohovací software | ANO / NE | …………………….……… |
| 4. | NAS zařízení | ANO / NE | …………………….……… |
| 5. | Vícefaktorové ověřování | ANO / NE | …………………….……… |
| 6. | Firewall | ANO / NE | …………………….……… |
| 7. | Záložní pásková knihovna | ANO / NE | …………………….……… |
| 8. | Monitoring IT infrastruktury | ANO / NE | …………………….……… |
| 9. | LOG management | ANO / NE | …………………….……… |
| 10. | Instalace a implementace | ANO / NE | …………………….……… |
| 11. | Zaškolení obsluhy | ANO / NE | …………………….……… |

**Prohlašuji**, že veškeré shora uvedené údaje (parametry) jsou úplné, pravdivé a odpovídají skutečnosti. Jsem si vědom/a právních následků v případě uvedení nesprávných nebo nepravdivých údajů (parametrů).

V **………………………..………,** dne **………….……**

**Osoba oprávněná jednat jménem/za účastníka:**

Titul, jméno, příjmení: **………………………………….…**

Funkce: **………………………………….…**