CENTRUM kociánka

Příloha č. 1 Smlouvy o dílo

IT služby (technika a hardware na pracovištích)

Přehled předmětné infrastruktury:

- Servery – vSphere HA Cluster, OS: ESXi, MS Windows Server DC, Linux
- Nutanix HCI Cluster
- VMware vSAN Advanced, all-flash, Dell EMC DataDomain
- Virtuální desktopy – Vmware Horizon View, 100x, terminály (ThinLinx OS a Stratodesk OS),
- Notebooky – 20ks, OS Microsoft Windows
- Virtuální servery – Vmware vSphere, 116VM, (OS Windows server a Linux)
- NETWORK – areál CK Brno, CK Březejc, optická + TP strukturovaná kabeláž + WiFi, cca 20x10gbit Aruba LAN Switch, 30x Aruba WIFI AP s centrálním managementem a řízenou bezpečností (guest access, klientská, zaměstnanecká síť, 802.1x radius), firewall, VMWare Velocloud - 3x Edge + 1x Gateway Edge,)
- Tiskárny – 40ks multifunkční laserová tiskárna Lexmark, centrální management, 3ks multifunkční tiskárny Minolta
- Monitoring a security
  - LOGmanager
  - FlowMon
  - BitDefender desktop antivir
  - BitDefender Grivity Zone pro virtuální infrastrukturu (servery a desktopy)
  - Identity Management Evolveum midPoint (s integrací Chytrá organizace, AD, Azure AD, Google ID)
- Zálohovací systém IBM Spectrum Protect s implementací Virtual Tape Library DELL DataDomain
- kancelářský sw Google Workspace

Prováděné činnosti nad kompletní předmětnou infrastrukturou:

- IT Podpora uživatelům v rozsahu pracovních dnů (8x5 8-16h)
- min 1 den z týdne přítomnost technika podpory fyzicky/prezenčně v lokalitě CK Brno a na vyžádání objednatele také na jiných pobočkách organizace v rámci ČR
- Hotline 24x7 – přijímání hlášení závad a požadavků, krátké telefonické a e-mail dotazy a konzultace
- Řešení hlášených poruch a havárií omezující provoz s garancí zahájení řešení poruchy v režimu 24x7, nejpozději do 4h od nahlášení
- Průběžná instalace doporučených bezpečnostních záplat
- Administrace a průběžná údržba
- Komunikace s výrobci SW a HW v případě řešení závad spadajících pod záruční či pozáruční servis výrobce HW/SW
- Pravidelný monitoring server/storage virtualizační infrastruktury (kontrola každý den), korekce odchylek od plynulého provozu
- Pravidelný monitoring infrastruktury VDI (kontrola každý den), korekce odchylek od plynulého provozu
- Pravidelný monitoring zálohování (kontrola každý den), korekce neúspěšných záloh, garance úspěšné obnovy
- Diagnostika při bezpečnostních nebo provozních incidentech – analýza dat z bezpečnostních nástrojů LOGmanager, Flowmon, antivir, firewall, velocloud.
- Navrhování bezpečnostních opatření a jejich zavádění do provozu.
- Udržování účinnosti a efektivity bezpečnostních ochran (firewall pravidla, politiky IT bezpečnosti, audit přidělování oprávnění uživatelům apod.)
- Vedení, udržování aktuálnosti a kompletnosti dokumentace IT
- Pravidelný Reporting o stavu, rozsahu a fungování služeb IT