6.7 Popis povinných parametrů dodávaného řešení

Komodita K1 - Rozšíření kapacit Technologického centra				
Část	**Parametr**	**Popis povinného parametru**	**Uchazeč popíše způsob naplnění tohoto povinného parametru včetně značkové specifikace nabízených dodávek**	**Uchazeč uvede odkaz na přiloženou část nabídky, kde je možné ověřit naplnění parametru**
Virtualizační server 1 ks BL460c G10	Provedení	Blade server	Blade server BL460c G10	Kapitola 6.1 Technické řešení
	Procesor	2x procesor osmi-jádrový (dohromady 16 jader), nominální frekvence min. 3.2 GHz, automatické zvýšení frekvence jádra až o 0,5 GHz při nevyužití ostatních jader)	2x procesor Xeon-G 6134 osmi-jádrový (dohromady 16 jader), nominální frekvence 3.2 GHz, automatické zvýšení frekvence jádra až o 0,5 GHz při nevyužití ostatních jader)	Kapitola 6.1 Technické řešení
	Pevné disky	2x SSD, min. 140 GB pro hypervizor	2x SSD, min. 240 GB pro hypervizor	Kapitola 6.1 Technické řešení
	Řadič disků	min. RAID 0,1, zálohovaná cache pro zápis min. 1 GB	min. RAID 0,1, zálohovaná cache pro zápis 1 GB	Kapitola 6.1 Technické řešení
	Paměť	minimálně 320 GB RAM, min. 2600 MT/s	10x 32GB 2Rx4 PC4-2666V-R Smart Kit celkem 320 GB RAM, 2666 MT/s	Kapitola 6.1 Technické řešení
	Rozšiřitelnost	rozšiřitelnost RAM min. na 700 GB bez výměny RAM modulů	rozšiřitelnost RAM na 700 GB bez výměny RAM modulů	Kapitola 6.1 Technické řešení
	RAID	řadič RAID 0,1, 10, zálohovaná vyrovnávací paměť pro zápis min. 1 GB	řadič RAID 0,1, 10, SAS 12 Gb, zálohovaná vyrovnávací paměť pro zápis min. 1 GB	Kapitola 6.1 Technické řešení
	LAN porty	LAN 2x10Gb s podporou iSCSI a virtualizace VMware NetQueue, Microsoft VMQ. Podpora partitioningu - rozdělení fyzického LAN adaptéru na více virtuálních adaptérů - min. 4 virtuální adaptéry na každý port	LAN 2x10Gb s podporou iSCSI a virtualizace VMware NetQueue, Microsoft VMQ. Podpora partitioningu - rozdělení fyzického LAN adaptéru na více virtuálních adaptérů - 4 virtuální adaptéry na každý port	Kapitola 6.1 Technické řešení
	FC porty	2x FC (fibre channel) port min. 16 Gb	2x FC (fibre channel) port 16 Gb	Kapitola 6.1 Technické řešení
	Vzdálená správa	Podpora vzdálené klávesnice, myši a obrazovky bez nutnosti běhu OS, možnost zapínat a vypínat server, možnost bootování se vzdáleného média.	Podpora vzdálené klávesnice, myši a obrazovky bez nutnosti běhu OS, možnost zapínat a vypínat server, možnost bootování se vzdáleného média.	Kapitola 6.1 Technické řešení
	Kompatibilita	Podpora nejrozšířenějších operačních systémů (Windows, Linux) a hypervizorů (Hyper-V, VMware)	Podpora nejrozšířenějších operačních systémů (Windows, Linux) a hypervizorů (Hyper-V, VMware)	Kapitola 6.1 Technické řešení
	Kompatibilita	Plně kompatibilní se stávajícím Blade šasi HP C7000 na fyzické i elektrické úrovni	Plně kompatibilní se stávajícím Blade šasi HP C7000 na fyzické i elektrické úrovni	Kapitola 6.1 Technické řešení
	Vysoká dostupnost	Podpora a licence pro clusterový provoz	Podpora a licence pro clusterový provoz	Kapitola 6.1 Technické řešení
	Management	Plná integrace s management modulem HP Blade šasi HP 7000	Plná integrace s management modulem HP Blade šasi HP 7000	Kapitola 6.1 Technické řešení
	Záruka	Záruka 60 měsíců, oprava následující pracovní den v místě instalace	Záruka 60 měsíců, oprava následující pracovní den v místě instalace – HPE Carepack	Kapitola 6.1 Technické řešení
SW licence operačních systémů	Operační systémy	Licence 64 - bitového serverového operačního systému v aktuální verzi pro nabízený server. Licence musí umožnit provoz neomezeného počtu virtuálních serverů stejné verze v prostředí stávající	Windows Server 2016 Datacenter 16 core - Licence 64 - bitového serverového operačního systému v aktuální verzi pro nabízený server. Licence umožňuje provoz neomezeného počtu virtuálních serverů stejné verze v	Kapitola 6.1 Technické řešení

Komodita K1 - Rozšíření kapacit Technologického centra				
Windows Server 2016 Datacenter 16 core		serverové virtualizace, dále provoz všech nabízených aplikací, management nástrojů.	prostředí stávající serverové virtualizace, dále provoz všech nabízených aplikací, management nástrojů a komponent terminálové farmy	
Síťové přepínače a sondy síťových toků 4 kusy 4x JC100B HPE 5800 24G Switch 2x JC091A HPE 5800 4-port 10GbE SFP+ Module 2x JC095A HPE 5800 16-port SFP Module	**Společné parametry**			
	Provedení	do racku, rozměr max. 1RU, včetně montážního materiálu do racku	do racku, rozměr 1RU, včetně montážního materiálu do racku	Kapitola 6.1 Technické řešení
	Určení	L2, L3 switch (přepínač), spravovatelný	L2, L3 switch (přepínač), spravovatelný	Kapitola 6.1 Technické řešení
	Porty	4x 10 GbSFP+, 16x 1 Gb SFP, 48x 1Gb RJ-45, optické a metalické porty nesdílené	4x 10 GbSFP+, 16x 1 Gb SFP, 48x 1Gb RJ-45, optické a metalické porty nesdílené	Kapitola 6.1 Technické řešení
	Podavač	podpora směrování a dynamických směrovacích protokolů (min. OSPF)	podpora směrování a dynamických směrovacích protokolů (min. OSPF)	Kapitola 6.1 Technické řešení
	VLAN	podpora min. 1000 aktivních VLAN a to včetně L3 směrovaných rozhraní	podpora 1000 aktivních VLAN a to včetně L3 směrovaných rozhraní	Kapitola 6.1 Technické řešení
	Routování	podpora tvorby virtuálních směrovacích tabulek (VRF, virtual router apod.)	podpora tvorby virtuálních směrovacích tabulek (VRF, virtual router apod.)	Kapitola 6.1 Technické řešení
	QoS	podpora QoS (min. 8 front na port)	podpora QoS (8 front na port)	Kapitola 6.1 Technické řešení
	Bezpečnost	podpora 802.1x	podpora 802.1x	Kapitola 6.1 Technické řešení
	Rozšířené funkce	podpora MPLS a VPLS, včetně routování pro napojení na MAN	podpora MPLS a VPLS, včetně routování pro napojení na MAN	Kapitola 6.1 Technické řešení
	IPV6	plný dual stack IPv4 a IPv6 včetně všech služeb směrování	plný dual stack IPv4 a IPv6 včetně všech služeb směrování	Kapitola 6.1 Technické řešení
	Výkon	přepínání a routování min. 200 Gb/s a 150 Mp/s	přepínání a routování 200 Gb/s a 150 Mp/s	Kapitola 6.1 Technické řešení
	Sledování toků	integrovaná podpora sledování toků technologie sFlow a exportu toků protokolem Netflow nebo kompatibilním.	integrovaná podpora sledování toků technologie sFlow a exportu toků protokolem Netflow nebo kompatibilním.	Kapitola 6.1 Technické řešení
	Stohování	podpora rozšířeného stohování po standardizovaných 10Gb portech do minimálního počtu 8 přepínačů (technologie ekvivalentní s technologiemi VSS, IRF nebo VirtualChasis)	podpora rozšířeného stohování po standardizovaných 10Gb portech do minimálního počtu 8 přepínačů (technologie ekvivalentní s technologiemi VSS, IRF nebo VirtualChasis)	Kapitola 6.1 Technické řešení
	Linková agregace	Agregace portů napříč stohem včetně kombinace 10 Gb a 1 Gb, podpora LACP	Agregace portů napříč stohem včetně kombinace 10 Gb a 1 Gb, podpora LACP	Kapitola 6.1 Technické řešení
	Správa	podpora SNMP, Syslog, CLI	podpora SNMP, Syslog, CLI	Kapitola 6.1 Technické řešení
	Záruka	Min. 5 let včetně nároku na nové verze firmware, oprava do 2 pracovních dnů v místě instalace	5 let včetně nároku na nové verze firmware, oprava do 2 pracovních dnů v místě instalace	Kapitola 6.1 Technické řešení
	Specifické parametry			
	Porty	2 přepínače - 4x 10 Gb SFP+, 16x 1 Gb SFP, 24x 1Gb RJ-45, optické a metalické porty nesdílené	2 přepínače - 4x 10 Gb SFP+, 16x 1 Gb SFP, 24x 1Gb RJ-45, optické a metalické porty nesdílené	Kapitola 6.1 Technické řešení
	Porty	2 přepínače - 8x 10 Gb SFP+, 24x 1Gb RJ-45, optické a metalické porty nesdílené	2 přepínače - 8x 10 Gb SFP+, 24x 1Gb RJ-45, optické a metalické porty nesdílené	Kapitola 6.1 Technické řešení
Kabely, optické moduly	Optické moduly	32x 1Gb SFP SM pro nabízené přepínače 8x 10 Gb SPF+ MM pro nabízené přepínače	32x 1Gb SFP SM pro nabízené přepínače 8x 10 Gb SPF+ MM pro nabízené přepínače	Kapitola 6.1 Technické řešení

Komodita K1 - Rozšíření kapacit Technologického centra				
		2x 10 Gb SPF+ SM BiDi, 10 km, pro nabízené přepínače, shodné vlnové délky 2x 10 Gb SPF+ SM BiDi, 10 km, pro stávající přepínače HPE 5130 (JG934A) - komplementární vlnové délky k předchozím modulům optický konektor modulů LC záruka min. 36 měsíců	2x 10 Gb SPF+ SM BiDi, 10 km, pro nabízené přepínače, shodné vlnové délky 2x 10 Gb SPF+ SM BiDi, 10 km, pro stávající přepínače HPE 5130 (JG934A) - komplementární vlnové délky k předchozím modulům optický konektor modulů LC záruka 36 měsíců	
	Kabely	4x optický patch kabel 3m MM - LC-LC 36x optický patch kabel 3m SM - LC-SC záruka min. 36 měsíců	4x optický patch kabel 3m MM - LC-LC 36x optický patch kabel 3m SM - LC-SC záruka 36 měsíců	Kapitola 6.1 Technické řešení
Rozšíření kapacity síťového úložiště NAS pro archivaci SIEM 12x HDD 4TB WD4002FFWX Red Pro 128MB SATAIII NAS	HDD	12x 4TB HDD SATAIII/128 MB cache. Disky musí být výrobcem určeny pro nepřetržitý provoz v NAS, nejsou přípustné disky určené pro jiné využití - např. desktopy, kamerové systémy apod.	12x 4TB HDD SATAIII/128 MB cache. Disky jsou výrobcem určeny pro nepřetržitý provoz v NAS,	Kapitola 6.1 Technické řešení
	Záruka	Záruka výrobce min. 5 let	Záruka výrobce 5 let	Kapitola 6.1 Technické řešení
Rozšíření kapacit diskových polí pro SIEM 6 ks HP HDD MDL 3TB GB / 7200 ot. min, SAS 6 Gb	HDD 3,5"	6 ks HDD MDL 3TB GB / 7200 ot. min, SAS min. 6 Gb	6 ks HP HDD MDL 3TB GB / 7200 ot. min, SAS 6 Gb	Kapitola 6.1 Technické řešení
	Kompatibilita	Plná kompatibilita s diskovými poli HP MSA 2000G3	Plná kompatibilita s diskovými poli HP MSA 2000G3	Kapitola 6.1 Technické řešení
	Záruka	Záruka min. 3 roky s výměnou v místě instalace	Záruka 3 roky s výměnou v místě instalace	Kapitola 6.1 Technické řešení

Komodita K2 -SIEM a NBA				
Část	**Parametr**	**Popis povinného parametru**	**Uchazeč popíše způsob naplnění tohoto povinného parametru včetně značkové specifikace nabízených dodávek**	**Uchazeč uvede odkaz na přiloženou část nabídky, kde je možné ověřit naplnění parametru**
SIEM & NBA	Základní funkce	Integrovaný systém pracování logů a událostí z definovaných zdrojů napříč výrobci aplikací, operačních systémů a síťového hardware a sledování síťových toků a detekce anomálií	Integrovaný systém pracování logů a událostí z definovaných zdrojů napříč výrobci aplikací, operačních systémů a síťového hardware a sledování síťových toků a detekce anomálií	Kapitola 6.1 Technické řešení

Komodita K2 -SIEM a NBA				
AlienVault Unified Security Manager	Ovládání	Uživatelsky přívětivý přístup ke všem komponentám systému z jednotného grafického uživatelského rozhraní (GUI). Konfigurace, definice zdrojů logů, definice korelačních pravidel, tvorba reportů, řešení událostí a další běžné operace musí probíhat z jediné řídící konzole s jednotným GUI.	Uživatelsky přívětivý přístup ke všem komponentám systému z jednotného grafického uživatelského rozhraní (GUI). Konfigurace, definice zdrojů logů, definice korelačních pravidel, tvorba reportů, řešení událostí a další běžné operace musí probíhat z jediné řídící konzole s jednotným GUI.	Kapitola 6.1 Technické řešení
	Správa prvků	Automatické jednorázové i plánovatelné vyhledávání i ruční přidávání Prvků a detekce jejich typů a vlastností. Prvkem se rozumí hw i sw (např. OS) s IP adresou. Prvky jsou typicky zdroji dat - logů a událostí.	Automatické jednorázové i plánovatelné vyhledávání i ruční přidávání Prvků a detekce jejich typů a vlastností. Prvkem se rozumí hw i sw (např. OS) s IP adresou. Prvky jsou typicky zdroji dat - logů a událostí.	Kapitola 6.1 Technické řešení
	Skupiny Prvků	Podpora zařazování Prvků do skupin/kategorií dle vlastností (typ, operační systém, dostupné služby, síť apod.) i metadat (umístění, hodnota apod.)	Podpora zařazování Prvků do skupin/kategorií dle vlastností (typ, operační systém, dostupné služby, síť apod.) i metadat (umístění, hodnota apod.)	Kapitola 6.1 Technické řešení
	Metadata Prvků	Možnost konfigurace metadat Prvku - min. hodnota, priorita a spolehlivost (věrohodnost) událostí	Možnost konfigurace metadat Prvku - min. hodnota, priorita a spolehlivost (věrohodnost) událostí	Kapitola 6.1 Technické řešení
	Monitorování Prvků	Automatické monitorování stavu Prvku - min. dostupnost poskytované služby a základní dostupnost (odezva na ping)	Automatické monitorování stavu Prvku - dostupnost poskytované služby a základní dostupnost (odezva na ping)	Kapitola 6.1 Technické řešení
	Vyhledávání Prvků	Víceparametrové vyhledávání a filtrování Prvků podle vlastností i metadat, export do souboru v běžném strojově zpracovatelném formátu (např. csv, xml apod.)	Víceparametrové vyhledávání a filtrování Prvků podle vlastností i metadat, export do souboru v běžném strojově zpracovatelném formátu (csv, xml apod.)	Kapitola 6.1 Technické řešení
	Vazby	Detekce síťových prvků standardními protokoly a mapovaní jejich vazeb	Detekce síťových prvků standardními protokoly a mapovaní jejich vazeb	Kapitola 6.1 Technické řešení
	Detekce zranitelností	Automatická ruční i plánovaná detekce zranitelností Prvků (i nezařazených) - porovnání stavu Prvků s databází známých zranitelností průběžně aktualizovanou výrobcem	Automatická ruční i plánovaná detekce zranitelností Prvků (i nezařazených) - porovnání stavu Prvků s databází známých zranitelností průběžně aktualizovanou výrobcem	Kapitola 6.1 Technické řešení
	Profily zranitelnosti	Vestavěné i uživatelsky definované profily detekce zranitelností – definice typů zranitelností, které mají být kontrolovány.	Vestavěné i uživatelsky definované profily detekce zranitelností – definice typů zranitelností, které mají být kontrolovány.	Kapitola 6.1 Technické řešení
	Autentizace	Podpora detekce zranitelností s i bez přihlášení (autentizací) ke kontrolovanému Prvku.	Podpora detekce zranitelností s i bez přihlášení (autentizací) ke kontrolovanému Prvku.	Kapitola 6.1 Technické řešení
	Detekce průniku	Víceúrovňová detekce průniku (intrusion detection) - min. na úrovni sledování síťového provozu a na úrovni Prvků.	Víceúrovňová detekce průniku (intrusion detection) - na úrovni sledování síťového provozu a na úrovni Prvků.	Kapitola 6.1 Technické řešení
	Instalace agentů	Podpora vzdálené instalace ID agentů (intrusion detection) min. pro operační systémy Microsoft Windows	Podpora vzdálené instalace ID agentů (intrusion detection) min. pro operační systémy Microsoft Windows	Kapitola 6.1 Technické řešení
	Detekce průniku – assety	Monitoring a analýza uživatelských aktivit, logů, integrity souborů a registrů, rootkitů či obdobného škodlivého kódu	Monitoring a analýza uživatelských aktivit, logů, integrity souborů a registrů, rootkitů či obdobného škodlivého kódu	Kapitola 6.1 Technické řešení
	Detekce průniku – síť	Analýza monitorovaných síťových toků a detekce anomálií indikující možné narušení bezpečnostní politiky (NBA - Network Behavior Analysis)	Analýza monitorovaných síťových toků a detekce anomálií indikující možné narušení bezpečnostní politiky (NBA - Network Behavior Analysis)	Kapitola 6.1 Technické řešení

Komodita K2 -SIEM a NBA				
	Detekce anomálií	Monitorování síťových toků technologií netflow (min. verze 5,9,10) či kompatibilní (ipfix, netstream) dle nabízených sond a přepínačů.	Monitorování síťových toků technologii netflow (verze 5,9,10) či kompatibilní (ipfix, netstream) dle nabízených sond a přepínačů.	Kapitola 6.1 Technické řešení
	Síťové toky hypervizor	Podpora sledování síťových toků (netflow či kompatibilní) virtuálních síťových přepínačů VMware vSphere	Podpora sledování síťových toků (netflow či kompatibilní) virtuálních síťových přepínačů VMware vSphere	Kapitola 6.1 Technické řešení
	Viditelnost síťových toků	Viditelnost síťového provozu - zobrazení, prohledávání, filtrování síťových toků včetně historie	Viditelnost síťového provozu - zobrazení, prohledávání, filtrování síťových toků včetně historie	Kapitola 6.1 Technické řešení
	IP reputace	Integrovaná služba aktualizovaná výrobcem ohodnocující reputaci a spolehlivost veřejné IP adresy s možností změny priorit událostí, alarmů apod. Reputace založena na detekovaných (aktivitách IP adresy (spam, skenování, phising, distribuce malware, botnet apod.	Integrovaná služba aktualizovaná výrobcem ohodnocující reputaci a spolehlivost veřejné IP adresy s možností změny priorit událostí, alarmů apod. Reputace založena na detekovaných (aktivitách IP adresy (spam, skenování, phising, distribuce malware, botnet	Kapitola 6.1 Technické řešení
	Protokoly	podporované protokoly min. syslog, windows events collection (pomocí agenta i bezagentově (např. WMI), snmp, s/ftp, nfs, cifs, netflow	podporované protokoly min. syslog, windows events collection (pomocí agenta i bezagentově (WMI), snmp, s/ftp, nfs, cifs, netflow	Kapitola 6.1 Technické řešení
	Ukládání logů	Bezpečné ukládání logů s řízeným přístupem v nezměněné (nefiltrované) podobě (tzv. raw logy)	Bezpečné ukládání logů s řízeným přístupem v nezměněné (nefiltrované) podobě (raw logy)	Kapitola 6.1 Technické řešení
	Zpracování logů	Centrální zpracování logů, jejich normalizace, korelaci, grafická interpretace a archivace, včetně logů generovaných samotným řešením	Centrální zpracování logů, jejich normalizace, korelaci, grafická interpretace a archivace, včetně logů generovaných samotným řešením	Kapitola 6.1 Technické řešení
	Rozšíření logů	Vytváření vlastních atributů v událostech. Automatické doplňování atributů aktuálními hodnotami z externího zdrojů. Podpora atributů v celém systému - vyhledávání, filtrace, korelace atd.	Vytváření vlastních atributů v událostech. Automatické doplňování atributů aktuálními hodnotami z externího zdrojů. Podpora atributů v celém systému - vyhledávání, filtrace, korelace atd.	Kapitola 6.1 Technické řešení
	Prohledávání logů	Pokročilé prohledávání a filtrování raw logů, podpora indexování pro zrychlení hledání	Pokročilé prohledávání a filtrování raw logů, podpora indexování pro zrychlení hledání	Kapitola 6.1 Technické řešení
	Expirace logů	Podpora automatické rotace raw logů s nastavením doby expirace	Podpora automatické rotace raw logů s nastavením doby expirace	Kapitola 6.1 Technické řešení
	Zálohování logů	Podpora zálohování logů na externí síťové úložiště	Podpora zálohování logů na externí síťové úložiště	Kapitola 6.1 Technické řešení
	Ochrana logů	Zajištění integrity raw logů aplikací digitální podpisu. Možnost jednoduchého uživatelského ověření integrity.	Zajištění integrity raw logů aplikací digitální podpisu. Možnost jednoduchého uživatelského ověření integrity.	Kapitola 6.1 Technické řešení
	Centralizace logů	Konsolidace logů na jednom centrálním místě.	Konsolidace logů na jednom centrálním místě.	Kapitola 6.1 Technické řešení
	Geolokace	Automatické doplňování geolokačních informací k událostem a jejich grafické znázornění na mapě	Automatické doplňování geolokačních informací k událostem a jejich grafické znázornění na mapě	Kapitola 6.1 Technické řešení
	Doplňování názvů	Automatické doplňování reverzních DNS a hostname záznamů k IP adresám.	Automatické doplňování reverzních DNS a hostname záznamů k IP adresám.	Kapitola 6.1 Technické řešení

Komodita K2 -SIEM a NBA				
	Indentifikace MAC	Automatické doplňování výrobce zařízení podle MAC adresy	Automatické doplňování výrobce zařízení podle MAC adresy	Kapitola 6.1 Technické řešení
	Grafy událostí	Grafické znázornění událostí - četnost, typ, časová osa	Grafické znázornění událostí - četnost, typ, časová osa	Kapitola 6.1 Technické řešení
	Parsery	Možnost vytváření uživatelských parserů bez nutnosti externí spolupráce	Možnost vytváření uživatelských parserů bez nutnosti externí spolupráce	Kapitola 6.1 Technické řešení
	Ladění parserů	On-line ladění uživatelsky vytvářených parserů v reálném čase-okamžité zobrazení rozparsovaných dat při vložení testovací zprávy/události.	On-line ladění uživatelsky vytvářených parserů v reálném čase-okamžité zobrazení rozparsovaných dat při vložení testovací zprávy/události.	Kapitola 6.1 Technické řešení
	Standardizace logů	Standardizace přijatých logů do jednotného formátu, parsování parametrů do předepsaných polí	Standardizace přijatých logů do jednotného formátu, parsování parametrů do předepsaných polí	Kapitola 6.1 Technické řešení
	Pohledy	Předpřipravené pohledy a podpora vytváření vlastních pohledů na data uživateli a jejich ukládání pro pozdější využití a zpracování dat. Včetně grafické reprezentace dat - grafy, mapy apod.	Předpřipravené pohledy a podpora vytváření vlastních pohledů na data uživateli a jejich ukládání pro pozdější využití a zpracování dat. Včetně grafické reprezentace dat - grafy, mapy	Kapitola 6.1 Technické řešení
	Reporty	Integrovaný reportovací nástroj s přednastavenými obvyklými reporty a možností vlastních úprav a vytvoření nových reportů. Včetně grafické reprezentace dat - grafy, mapy apod.	Integrovaný reportovací nástroj s přednastavenými obvyklými reporty a možností vlastních úprav a vytvoření nových reportů. Včetně grafické reprezentace dat - grafy, mapy	Kapitola 6.1 Technické řešení
	Upozornění	Zasílání uživatelsky vytvořených upozornění podle uživatelsky definovaných podmínek. Možnost zahrnutí přijatých rozparsovaných dat do upozornění.	Zasílání uživatelsky vytvořených upozornění podle uživatelsky definovaných podmínek. Možnost zahrnutí přijatých rozparsovaných dat do upozornění.	Kapitola 6.1 Technické řešení
	Správa uživatelů	Správa uživatelů systému musí umožnit integraci s MS Active Directory. Systém musí umožňovat i přihlašování pomocí lokálních účtů. Podpora granulárního (lokálního) nastavení uživatelských oprávnění.	Správa uživatelů systému musí umožnit integraci s MS Active Directory. Systém musí umožňovat i přihlašování pomocí lokálních účtů. Podpora granulárního (lokálního) nastavení uživatelských oprávnění.	Kapitola 6.1 Technické řešení
	Tikety	Možnost vytváření tiketů k bezpečnostním událostem s možností přiřazení řešiteli. Možnost sledování průběhu tiketů včetně historie - obsah, vykonané činnosti, eskalace. Podpora jednoduchého manuálního vytváření tiketů v průběhu vyšetřování incidentu.	Možnost vytváření tiketů k bezpečnostním událostem s možností přiřazení řešiteli. Možnost sledování průběhu tiketů včetně historie - obsah, vykonané činnosti, eskalace. Podpora jednoduchého manuálního vytváření tiketů v průběhu vyšetřování incidentu.	Kapitola 6.1 Technické řešení
	Automatizace tiketů	Tickety lze vytvářet automaticky na základě vytvořené politiky k jednotlivým událostem / zranitelnostem.	Tickety lze vytvářet automaticky na základě vytvořené politiky k jednotlivým událostem / zranitelnostem.	Kapitola 6.1 Technické řešení
	Politiky	Podpora vestavěných a tvorby vlastních komplexních politik zpracování událostí. Politiky musí umožnit spustit minimálně následující akce: odeslání emailu, vytvoření ticketu, spuštění skriptu.	Podpora vestavěných a tvorby vlastních komplexních politik zpracování událostí. Politiky umožní spustit následující akce: odeslání emailu, vytvoření ticketu, spuštění skriptu.	Kapitola 6.1 Technické řešení
	Korelace	Podpora korelací události na základě definovaných parametru bez závislosti na typu zdroje. Vestavěné a výrobcem aktualizované korelace, podpora vytváření vlastních	Podpora korelací události na základě definovaných parametru bez závislosti na typu zdroje. Vestavěné a výrobcem aktualizované korelace, podpora vytváření vlastních	Kapitola 6.1 Technické řešení

Komodita K2 -SIEM a NBA				
	Rozšířené korelace	Systém musí umožňovat tvorbu korelací nejen napříč zdroji, ale také napříč daty z interních subsystémů (např. detekce zranitelnosti, průniků, IP reputace). V závislosti na datech interních subsystémů je případně upravena vážnost incidentu (oproti standardní korelaci).	Systém umožní tvorbu korelací nejen napříč zdroji, ale také napříč daty z interních subsystémů (detekce zranitelnosti, průniků, IP reputace). V závislosti na datech interních subsystémů je případně upravena vážnost incidentu (oproti standardní korelaci).	Kapitola 6.1 Technické řešení
	Upozornění	Podpora vytvářet upozornění (alertů) na základě korelovaných událostí včetně zahrnutí rozšířených korelací. Vestavěná upozornění i podpora ručního vytváření.	Podpora vytvářet upozornění (alertů) na základě korelovaných událostí včetně zahrnutí rozšířených korelaci. Vestavěná upozornění i podpora ručního vytváření.	Kapitola 6.1 Technické řešení
	IT Compliance	Podpora compliance (jednání v souladu s „pravidly") - certifikace dle obvyklých bezpečnostních standardů a norem PCI DSS, HIPAA	Podpora compliance (jednání v souladu s „pravidly") - certifikace dle obvyklých bezpečnostních standardů a norem PCI DSS, HIPAA	Kapitola 6.1 Technické řešení
	Auditní reporty	Vestavěné, výrobcem aktualizované šablony reportů pro podporů kontrolních a certifikačních auditů - min. dle standardů PCI DSS, HIPAA, NIST CSF, ISO 27001	Vestavěné, výrobcem aktualizované šablony reportů pro podporů kontrolních a certifikačních auditů - dle standardů PCI DSS, HIPAA, NIST CSF, ISO 27001	Kapitola 6.1 Technické řešení
	Legislativa	Systém musí zajistit bezpečné, úplné a nezpochybnitelné ukládání, vyhodnocování a archivaci logů ICT prostředí zadavatele a naplnění požadavků dle zákona č. 181/2014 Sb. (ZKB) a vyhlášky č.316/2014 Sb. (VKB), o kybernetické bezpečnosti, a to v platných zněních	Systém zajistí bezpečné, úplné a nezpochybnitelné ukládání, vyhodnocování a archivaci logů ICT prostředí zadavatele a naplnění požadavků dle zákona č. 181/2014 Sb. (ZKB) a vyhlášky č.316/2014 Sb. (VKB), o kybernetické bezpečnosti, a to v platných zněních	Kapitola 6.1 Technické řešení
	Provedení	Centrální část systému bude realizována jako jedna virtuální appliance	Centrální část systému bude realizována jako jedna virtuální appliance	Kapitola 6.1 Technické řešení
	Licence	Licence pro neomezený počet sledovaných systémů (Prvků), bez licenčního omezení velikosti aktivních i archivních dat či jiných funkcionalit systému. Součástí licence bude centrální část systému a dále samostatný (sub)systém (virtuální appliance) zajišťující sběr dat a vykonávání funkcí systému (např. detekci Prvků, testy zranitelností, monitoring síťových tok, aběr logů atd.) lokálně ve vzdálené lokalitě (U spořitelny) a předávání dat a událostí do centrální části systému).	Licence pro neomezený počet sledovaných systémů (Prvků), bez licenčního omezení velikosti aktivních i archivních dat či jiných funkcionalit systému. Součástí licence bude centrální část systému a dále samostatný (sub)systém (virtuální appliance) zajišťující sběr dat a vykonávání funkcí systému (detekci Prvků, testy zranitelností, monitoring síťových tok, aběr logů) lokálně ve vzdálené lokalitě (U spořitelny) a předávání dat a událostí do centrální části systému).	Kapitola 6.1 Technické řešení
	Výkon	Trvalé zpracování AIO 1500 EPS (events per second - událostí za sekundu) - celkem z obou lokalit - Moskevská a U spořitelny	Trvalé zpracování AIO 1500 EPS (events per second - události za sekundu) - celkem z obou lokalit - Moskevská a U spořitelny	Kapitola 6.1 Technické řešení
	Škálovatelnost	Možnost zvýšení výkonu doplněním dalších appliance pro sběr dat a vykovávání funkcí systémů, popřípadě rozdělením systému na více serverů.	Možnost zvýšení výkonu doplněním dalších appliance pro sběr dat a vykovávání funkcí systémů, popřípadě rozdělením systému na více serverů.	Kapitola 6.1 Technické řešení
	Vysoká dostupnost	Integrovaná podpora pro možnost doplnění dalšího systému (nodu) a sestavení clusteru – min. 2 systém min, režim active/passive	Integrovaná podpora pro možnost doplnění dalšího systému (nodu) a sestavení clusteru – 2 systém, režim active/passive	Kapitola 6.1 Technické řešení

Komodita K2 -SIEM a NBA				
	Záruka	Min. 12 měsíců včetně nároku na nové verze software a včetně aktualizací bezpečnostní a funkčních signatur (zranitelnosti, korelační pravidla, detekce průniku, detekce Prvků (typy zařízení, aplikace, operační systémy), aktualizací reportů popř. další.	12 měsíců včetně nároku na nové verze software a včetně aktualizací bezpečnostní a funkčních signatur (zranitelnosti, korelační pravidla, detekce průniku, detekce Prvků (typy zařízení, aplikace, operační systémy), aktualizací reportů.	Kapitola 6.1 Technické řešení

Komodita K3 - Správa identit				
Část	**Parametr**	**Popis povinného parametru**	**Uchazeč popíše způsob naplnění tohoto povinného parametru včetně značkové specifikace nabízených dodávek**	**Uchazeč uvede odkaz na přiloženou část nabídky, kde je možné ověřit naplnění parametru**
Systém pro správu identity (Identity management - IDM) AC Identita	Základní funkce	IDM (dále IDM nebo Systém) bude udržovat a spravovat identity a organizační strukturu organizace. Spravované identity budou sloužit jako referenční identity pro ostatní vnitřní i vnější informační systémy. Identity budou ukládány v databázi.	IDM (dále IDM nebo Systém) bude udržovat a spravovat identity a organizační strukturu organizace. Spravované identity budou sloužit jako referenční identity pro ostatní vnitřní i vnější informační systémy. Identity budou ukládány v databázi.	Kapitola 6.1 Technické řešení
	Licence	Poskytnutá licence umožní nasazení a provoz IDM bez omezení na počet uživatelů, spravovaných identit a napojených systémů. Nejsou přípustná žádná další omezení omezující obvyklé nasazení a provoz s ohledem na charakter organizace Zadavatele (počet záznamů, velikost databází atd.). Předpokládaný počet uživatelů je do 500.	Poskytnutá licence umožní nasazení a provoz IDM bez omezení na počet uživatelů, spravovaných identit a napojených systémů. Nejsou přípustná žádná další omezení omezující obvyklé nasazení a provoz s ohledem na charakter organizace Zadavatele (počet záznamů, velikost databází). Předpokládaný počet uživatelů je do 500.	Kapitola 6.1 Technické řešení
	Škálovatelnost	Systém musí umožnit zvyšování výkonu (zlepšování odezvy) rozložením komponent Systému na více serverů - minimálně oddělení rolí (serverů) uživatelského rozhraní od výkonu integračních a provozních úloh.	Systém musí umožnit zvyšování výkonu (zlepšování odezvy) rozložením komponent Systému na více serverů - minimálně oddělení rolí (serverů) uživatelského rozhraní od výkonu integračních a provozních úloh.	Kapitola 6.1 Technické řešení
	Evidence aplikací a rolí	Integrovaný registr aplikací a informačních systémů (souhrnně IS) a jejich uživatelských rolí včetně možnosti importu rolí přes webové služby.	Integrovaný registr aplikací a informačních systémů (souhrnně IS) a jejich uživatelských rolí včetně možnosti importu rolí přes webové služby.	Kapitola 6.1 Technické řešení
	Uživatelské role	Integrovaná správa uživatelských rolí, včetně zařazení uživatele do odpovídající role v příslušných IS.	Integrovaná správa uživatelských rolí, včetně zařazení uživatele do odpovídající role v příslušných IS.	Kapitola 6.1 Technické řešení
	Historizace	Vestavěná detailní databázové historizace pro evidenci změn identit včetně referenčních objektů a vazeb mezi nimi. Historizace poskytne data v libovolném časovém okamžiku - aktuálním nebo zpětně v minulosti.	Vestavěná detailní databázové historizace pro evidenci změn identit včetně referenčních objektů a vazeb mezi nimi. Historizace poskytne data v libovolném časovém okamžiku - aktuálním nebo zpětně v minulosti.	Kapitola 6.1 Technické řešení
	Automatizace	Podpora intuitivní tvorby pravidel v grafickém prostředí pro automatické vytváření uživatelských účtů, začleňování uživatelů do skupin a přiřazování aplikačních rolí uživatelům na základě libovolných atributů identity a přidružených referenčních objektů (organizační jednotka, aplikační role, systematizované místo atd.).	Podpora intuitivní tvorby pravidel v grafickém prostředí pro automatické vytváření uživatelských účtů, začleňování uživatelů do skupin a přiřazování aplikačních rolí uživatelům na základě libovolných atributů identity a přidružených referenčních objektů (organizační jednotka, aplikační role, systematizované místo).	Kapitola 6.1 Technické řešení
	Logování SIEM	Systém bude poskytovat auditní logy pro systém typu SIEM	Systém bude poskytovat auditní logy pro systém typu SIEM	Kapitola 6.1 Technické řešení

Komodita K3 - Správa identit				
	Logování systému	Systém obsahuje logování min. následujících typů událostí: - události systému (aplikační log) - změny entit evidovaných systémem a změny konfigurace systému (auditni log) - synchronizace s napojenými systémy (synchronizační log) - odeslané notifikace a upozornění (notifikační log)	Systém obsahuje logování následujících typů událostí: - události systému (aplikační log) - změny entit evidovaných systémem a změny konfigurace systému (auditní log) - synchronizace s napojenými systémy (synchronizační log) - odeslané notifikace a upozornění (notifikační log)	Kapitola 6.1 Technické řešení
	Správa identit	Systém bude spravovat organizační strukturu obsahující interní a externí identity jako samostatné větve struktury.	Systém bude spravovat organizační strukturu obsahující interní a externí identity jako samostatné větve struktury.	Kapitola 6.1 Technické řešení
	Systematizovaná místa	Systém bude implementovat princip systemizovaných míst. Umožní systemizaci pracovních míst v souladu se strukturou organizace a bude spravovat jednotlivá systematizovaná místa a sadu oprávnění a rolí pro jednotlivé IS organizace vztažené ke konkrétnímu systemizovanému místu.	Systém bude implementovat princip systemizovaných míst. Umožní systemizaci pracovních míst v souladu se strukturou organizace a bude spravovat jednotlivá systematizovaná místa a sadu oprávnění a rolí pro jednotlivé IS organizace vztažené ke konkrétnímu systemizovanému místu.	Kapitola 6.1 Technické řešení
	Podpora eIDAS	Systém umožní implementaci procesů a rozhraní, která jsou vyžadována v Nařízení Evropského parlamentu a Rady (EU) č. 910/2014 ze dne 23. července 2014 o elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce na vnitřním trhu a o zrušení směrnice 1999/93/ES.	Systém umožní implementaci procesů a rozhraní, která jsou vyžadována v Nařízení Evropského parlamentu a Rady (EU) č. 910/2014 ze dne 23. července 2014 o elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce na vnitřním trhu a o zrušení směrnice 1999/93/ES.	Kapitola 6.1 Technické řešení
	Vysoká dostupnost	Systém musí být možno nasadit na více serverů v režimu vysoké dostupnosti.	Systém bude možno nasadit na více serverů v režimu vysoké dostupnosti.	Kapitola 6.1 Technické řešení
	Požadavky na portál - obecné	IDM bude obsahovat webový portál (dále jen Portál), který bude sloužit jako hlavní rozhraní pro uživatele i správce pro přístup k datům, funkcím, správu a konfiguraci Systému.	IDM bude obsahovat webový portál (dále jen Portál), který bude sloužit jako hlavní rozhraní pro uživatele i správce pro přístup k datům, funkcím, správu a konfiguraci Systému.	Kapitola 6.1 Technické řešení
	Podpora mobilních zařízení	Portál bude implementován s responzivním designem (přizpůsobení vzhledu typu zařízení, ze kterého je k portálu přistupováno)	Portál bude implementován s responzivním designem (přizpůsobení vzhledu typu zařízení, ze kterého je k portálu přistupováno)	Kapitola 6.1 Technické řešení
	Správa referenčních objektů	Portál bude umožňovat přehlednou správu samostatných identifikovatelných objektů - referenčních objektů, na které se identity mohou odkazovat: min. systematizované místo, organizační jednotka, skupina, agenda, agendová činnostní role, aplikace, skupina aplikací, aplikační role, certifikát.	Portál bude umožňovat přehlednou správu samostatných identifikovatelných objektů - referenčních objektů, na které se identity mohou odkazovat: systematizované místo, organizační jednotka, skupina, agenda, agendová činnostní role, aplikace, skupina aplikací, aplikační role, certifikát.	Kapitola 6.1 Technické řešení
	Referenční objekty	Systém umožní přidávání a správu dalších typů referenčních objektů a to i v průběhu správy konkrétní identity s možností okamžitého použití referenčního objektu u spravované identity	Systém umožní přidávání a správu dalších typů referenčních objektů a to i v průběhu správy konkrétní identity s možností okamžitého použití referenčního objektu u spravované identity	Kapitola 6.1 Technické řešení
	Zabezpečení referenčních objektů	Systém umožní nastavení samostatných nezávislých administrátorských oprávnění pro správu jednotlivých referenčních objektů	Systém umožní nastavení samostatných nezávislých administrátorských oprávnění pro správu jednotlivých referenčních objektů	Kapitola 6.1 Technické řešení

Komodita K3 - Správa identit				
	Rozšiřující atributy	Systém umožní dodatečné rozšiřování identit a referenčních objektů o další atributy a zajistí publikaci těchto nových atributů externím aplikacím prostřednictvím rozhraní webových služeb IDM.	Systém umožní dodatečné rozšiřování identit a referenčních objektů o další atributy a zajistí publikaci těchto nových atributů externím aplikacím prostřednictvím rozhraní webových služeb IDM.	Kapitola 6.1 Technické řešení
	Přehledné zobrazení	Portál umožní grafické zobrazení a současné vyhledávání identit / uživatelských účtů ve stromové organizační struktuře a prohledávání organizační struktury včetně systematizovaných míst až do úrovně jednotlivých uživatelských účtů (identit).	Portál umožní grafické zobrazení a současné vyhledávání identit / uživatelských účtů ve stromové organizační struktuře a prohledávání organizační struktury včetně systematizovaných míst až do úrovně jednotlivých uživatelských účtů (identit).	Kapitola 6.1 Technické řešení
	Vyhledávání - diakritika	Portál bude umožňovat vyhledávat i bez diakritiky (např. zadání Parizek vyhledává i Pařízek apod.)	Portál bude umožňovat vyhledávat i bez diakritiky (zadání Parizek vyhledává i Pařízek	Kapitola 6.1 Technické řešení
	Správa certifikátů	Správa uživatelů (identit) bude umožňovat i správu údajů o uživatelských digitálních certifikátech. Data o certifikátech bude možné nahrávat do systému prostřednictvím rozhraní webových služeb. Systém umožní automatické zneplatnění uložených certifikátů po vypršení data platnosti.	Správa uživatelů (identit) bude umožňovat i správu údajů o uživatelských digitálních certifikátech. Data o certifikátech bude možné nahrávat do systému prostřednictvím rozhraní webových služeb. Systém umožní automatické zneplatnění uložených certifikátů po vypršení data platnosti.	Kapitola 6.1 Technické řešení
	Obrázky	Systém umožní k jednotlivým účtům (identitám) přikládat obrázky - fotografie.	Systém umožní k jednotlivým účtům (identitám) přikládat obrázky - fotografie.	Kapitola 6.1 Technické řešení
	Přesun identit	Systém umožní přesun identit mezi jednotlivými organizacemi či jejich odděleními.	Systém umožní přesun identit mezi jednotlivými organizacemi či jejich odděleními.	Kapitola 6.1 Technické řešení
	Kopírování rolí	Systém umožní kopírovaní aplikačních rolí, agendových činnostních rolí mezi jednotlivými systematizovanými místy.	Systém umožní kopírovaní aplikačních rolí, agendových činnostních rolí mezi jednotlivými systematizovanými místy.	Kapitola 6.1 Technické řešení
	Ochrana proti chybám	Systém bude obsahovat mechanismus zabránění hromadným změnám z důvodu případných chybných vstupních dat (např. z personálního systému), aby nedošlo k hromadným nežádoucím změnám (například smazání objektů v Active Directory apod).	Systém bude obsahovat mechanismus zabránění hromadným změnám z důvodu případných chybných vstupních dat (např. z personálního systému), aby nedošlo k hromadným nežádoucím změnám (například smazání objektů v Active Directory)	Kapitola 6.1 Technické řešení
	Aktivní uživatelé	Systém bude obsahovat přehled uživatelů aktuálně pracujících s Portálem	Systém bude obsahovat přehled uživatelů aktuálně pracujících s Portálem	Kapitola 6.1 Technické řešení
	Slučování identit	Systém umožní sjednocení více uživatelů (identit) do jedné a odpovídající sjednocení spravovaných účtů.	Systém umožní sjednocení více uživatelů (identit) do jedné a odpovídající sjednocení spravovaných účtů.	Kapitola 6.1 Technické řešení
	Export údajů	Vestavěný export přehledů a seznamů zobrazených na portále do souborů CSV nebo obdobného strojově zpracovatelného a současně běžně čitelného formátu	Vestavěný export přehledů a seznamů zobrazených na portále do souborů CSV nebo obdobného strojově zpracovatelného a současně běžně čitelného formátu	Kapitola 6.1 Technické řešení
	Filtrování	Vestavěný editor filtrů pro vyhledávání identit a referenčních identit. Možnost filtrování libovolných atributů identity včetně přidružených referenčních objektů. Možnost uložení filtrů pro opakované použití.	Vestavěný editor filtrů pro vyhledávání identit a referenčních identit. Možnost filtrování libovolných atributů identity včetně přidružených referenčních objektů. Možnost uložení filtrů pro opakované použití.	Kapitola 6.1 Technické řešení
	Správa oprávnění	Víceúrovňová správa administrátorských oprávnění s možností nastavení oprávnění min. na úrovni organizační jednotky (nebo	Víceúrovňová správa administrátorských oprávnění s možností nastavení oprávnění min. na úrovni organizační jednotky (nebo	Kapitola 6.1 Technické řešení

Komodita K3 - Správa identit				
		hlouběji) a detailní přiřazení rolí a oprávnění (např. přiřazení činnostní role, přiřazení aplikační role, editace identity apod.)	hlouběji) a detailní přiřazení rolí a oprávnění (např. přiřazení činnostní role, přiřazení aplikační role, editace identity)	
	Granularita oprávnění	Oprávnění přidělovaná uživatelům a správcům bude možné definovat a přidělovat pro jednotlivé části systému (identity, referenční objekty, notifikací, synchronizací, konfigurace systému, reporty, workflow, webové služby atd.). U jednotlivých částí bude možnost definovat akce, které může uživatel s přidělenými oprávněními v konkrétní části IDM provádět.	Oprávnění přidělovaná uživatelům a správcům bude možné definovat a přidělovat pro jednotlivé části systému (identity, referenční objekty, notifikací, synchronizací, konfigurace systému, reporty, workflow, webové služby atd.). U jednotlivých částí bude možnost definovat akce, které může uživatel s přidělenými oprávněními v konkrétní části IDM provádět.	Kapitola 6.1 Technické řešení
	Oprávnění k atributům	Pro identity a referenčních objektů bude možná definovat oprávnění k jejich atributům včetně možností zobrazení / nezobrazení daného atributu, možnosti editace atributu uživatelem, povinnosti nastavení/vyplnění atributu, pořadí zobrazení atributů.	Pro identity a referenčních objektů bude možná definovat oprávnění k jejich atributům včetně možností zobrazení / nezobrazení daného atributu, možnosti editace atributu uživatelem, povinnosti nastavení/vyplnění atributu, pořadí zobrazení atributů.	Kapitola 6.1 Technické řešení
	Kontextový výběr	Na úrovní organizační jednotky bude možné pro výběr a přiřazování rolí nastavit sady povolených aplikační rolí, skupiny, agendových rolí, systematizovaných míst dostupných pro identity z dané organizační jednotky.	Na úrovni organizační jednotky bude možné pro výběr a přiřazování rolí nastavit sady povolených aplikační rolí, skupiny, agendových rolí, systematizovaných míst dostupných pro identity z dané organizační jednotky.	Kapitola 6.1 Technické řešení
	Správa licencí	IDM umožní spravovat licence pro jednotlivé evidované aplikace a přiřazovat je jednotlivým uživatelům (identitám). Pro schvalování přiřazování licencí bude IDM obsahovat workflow platformu s možností vytváření víceúrovňových schvalovacích workflow.	IDM umožní spravovat licence pro jednotlivé evidované aplikace a přiřazovat je jednotlivým uživatelům (identitám). Pro schvalování přiřazování licencí bude IDM obsahovat workflow platformu s možností vytváření víceúrovňových schvalovacích workflow.	Kapitola 6.1 Technické řešení
	Časová omezení	IDM bude umožňovat přiřazení rolí konkrétní identitě, systemizovanému místu, skupině a organizační jednotce včetně možnosti nastavení data a času vypršení platnosti přiřazení. Po vypršení platnosti přiřazení IDM rolí přiřazenému objektu automaticky odebere.	IDM bude umožňovat přiřazení rolí konkrétní identitě, systemizovanému místu, skupině a organizační jednotce včetně možnosti nastavení data a času vypršení platnosti přiřazení. Po vypršení platnosti přiřazení IDM rolí přiřazenému objektu automaticky odebere.	Kapitola 6.1 Technické řešení
	Vícenásobné vazby	Možnost přiřazení identit k systematizovaným místům ve vazbě M:N. Identita může být v IDM evidována na více systematizovaných místech a současně na systematizovaném místě může být evidováno více identit.	Možnost přiřazení identit k systematizovaným místům ve vazbě M:N. Identita může být v IDM evidována na více systematizovaných místech a současně na systematizovaném místě může být evidováno více identit.	Kapitola 6.1 Technické řešení
	Přehled rolí	Možnost zobrazení přidělených rolí k jednotlivým identitám s přehledným rozlišením rolí navázaných na systemizované místo, rolí navázaných na identitu, rolí navázaných na organizační jednotku, rolí navázaných na skupinu a delegovaných role.	Možnost zobrazení přidělených rolí k jednotlivým identitám s přehledným rozlišením rolí navázaných na systemizované místo, rolí navázaných na identitu, rolí navázaných na organizační jednotku, rolí navázaných na skupinu a delegovaných role.	Kapitola 6.1 Technické řešení

Komodita K3 - Správa identit				
	Přehled dědičností	IDM umožní evidenci a přehledné souhrnné zobrazení všech rolí včetně informace, odkud uživatel roli zdědil (z organizační jednotky, systematizovaného místa, skupiny) nebo zda má nějakou roli od někoho delegovánu.	IDM umožní evidenci a přehledné souhrnné zobrazení všech rolí včetně informace, odkud uživatel roli zdědil (z organizační jednotky, systematizovaného místa, skupiny) nebo zda má nějakou roli od někoho delegovánu.	Kapitola 6.1 Technické řešení
	Skupiny	IDM bude obsahovat správu skupin s možností začleňovat více skupin do sebe, přiřazovat do skupin jednotlivé uživatele i systematizovaná místa.	IDM bude obsahovat správu skupin s možností začleňovat více skupin do sebe, přiřazovat do skupin jednotlivé uživatele i systematizovaná místa.	Kapitola 6.1 Technické řešení
	Zastupitelnost	IDM bude obsahovat správu vztahů zastupitelnosti mezi uživateli. Musí umožnit uživatelům, aby v souladu se strukturou organizace mohli uživatelé delegovat v případě potřeby (dovolená, služební cesta) svoje role, nebo jejich část na jiné pověřené osoby a to i v režimu, kdy jeden uživatel může mít pro každou svou činnost nastaveného jiného uživatele jako zástupce.	IDM bude obsahovat správu vztahů zastupitelnosti mezi uživateli. Musí umožnit uživatelům, aby v souladu se strukturou organizace mohli uživatelé delegovat v případě potřeby (dovolená, služební cesta) svoje role, nebo jejich část na jiné pověřené osoby a to i v režimu, kdy jeden uživatel může mít pro každou svou činnost nastaveného jiného uživatele jako zástupce.	Kapitola 6.1 Technické řešení
	Delegování oprávnění	Možnost delegování administrátorských práv.	Možnost delegování administrátorských práv.	Kapitola 6.1 Technické řešení
	Správa osobních údajů	IDM umožní správu evidence osobních údajů - bude obsahovat správu evidence subjektů údajů a evidenci jejich osobních údajů včetně jejich kategorií a klasifikací.	IDM umožní správu evidence osobních údajů - bude obsahovat správu evidence subjektů údajů a evidenci jejich osobních údajů včetně jejich kategorií a klasifikací.	Kapitola 6.1 Technické řešení
	Osobní údaje	IDM bude obsahovat evidenci účelů pro nakládání s osobnímu údaji subjektů údajů. V rámci daného účelu budou definována oprávnění, aplikační role pro přístup k osobním údajům.	IDM bude obsahovat evidenci účelů pro nakládání s osobnímu údaji subjektů údajů. V rámci daného účelu budou definována oprávnění, aplikační role pro přístup k osobním údajům.	Kapitola 6.1 Technické řešení
	Osobní údaje - automatizace	IDM bude obsahovat workflow pro správu životního cyklu osobních údajů subjektu údajů.	IDM bude obsahovat workflow pro správu životního cyklu osobních údajů subjektu údajů.	Kapitola 6.1 Technické řešení
	Obnovení hesla	IDM bude obsahovat samoobslužné uživatelské rozhraní pro reset hesla jednotlivých účtů daného uživatele. Zasílání kódů pro reset hesla danému uživatele musí být možnou provádět pomocí SMS (tj. IDM musí být možné na SMS bránu či službu napojit). Rozhraní musí umožnit i běžnou změnu hesla (bez resetu).	IDM bude obsahovat samoobslužné uživatelské rozhraní pro reset hesla jednotlivých účtů daného uživatele. Zasílání kódů pro reset hesla danému uživatele musí být možnou provádět pomocí SMS (tj. IDM musí být možné na SMS bránu či službu napojit). Rozhraní musí umožnit i běžnou změnu hesla (bez resetu).	Kapitola 6.1 Technické řešení
	Žádosti	IDM bude obsahovat samoobslužné uživatelské rozhraní pro zadávání žádostí o přidělení jednotlivých aplikačních rolí a členství ve skupinách. Role a skupiny budou kategorizovány a kategoriím bude možné přidělit schvalovací workflow nebo může žádost vyřízena automaticky bez schválení.	IDM bude obsahovat samoobslužné uživatelské rozhraní pro zadávání žádostí o přidělení jednotlivých aplikačních rolí a členství ve skupinách. Role a skupiny budou kategorizovány a kategoriím bude možné přidělit schvalovací workflow nebo může žádost vyřízena automaticky bez schválení.	Kapitola 6.1 Technické řešení
	Externí subjekty	IDM bude obsahovat samoobslužné uživatelské rozhraní s konfigurovatelnými registračními formuláři pro registraci externích organizací a identit i jejich žádostí o konkrétní aplikační role nebo přiřazení do skupin.	IDM bude obsahovat samoobslužné uživatelské rozhraní s konfigurovatelnými registračními formuláři pro registraci externích organizací a identit i jejich žádostí o konkrétní aplikační role nebo přiřazení do skupin.	Kapitola 6.1 Technické řešení

Komodita K3 - Správa identit				
	Kontextový výběr	Samoobslužné rozhraní umožní na úrovni organizace a organizační jednotky definovat seznam rolí a skupin, o které mohou žadatelé požádat.	Samoobslužné rozhraní umožní na úrovni organizace a organizační jednotky definovat seznam rolí a skupin, o které mohou žadatelé požádat.	Kapitola 6.1 Technické řešení
	Individualizace	IDM umožní uživatelům individuálně nastavit vlastní zobrazení rozhraní - min. zobrazení / skrytí sloupců u všech seznamů, počet zobrazených záznamů na stránku - vždy pro každý seznam samostatně	IDM umožní uživatelům individuálně nastavit vlastní zobrazení rozhraní - min. zobrazení / skrytí sloupců u všech seznamů, počet zobrazených záznamů na stránku - vždy pro každý seznam samostatně	Kapitola 6.1 Technické řešení
	Workflow	Integrované workflow pro řízení životního cyklu změn identit a schvalování změn. Funkční požadavky: - Zadávání požadavků uživatelů na změny v přiřazení rolí a skupin ke schválení nadřízeným - Možnost sledování stavu svých požadavků uživateli - E-mailové upozornění schvalovatele na požadavek ke schválení - Přehled úloh ke schválení pro každého schvalovatele - Schvalování či zamítnutí požadavků včetně uvedení zdůvodnění - Podporova vícekrokového schvalování - Podpora schvalování jedním nebo více schvalovateli (skupinou schvalovatelů) - Správce IDM může pracovat se všemi úlohami - Možnost větvení pro ošetření výjimek vzniklých při schvalování - Řešení zastupitelnosti - Eskalace - upozornění při překročení termínu splnění - Možnost vkládání systémových kroků s voláním webových služeb a spuštěním skriptů	Integrované workflow pro řízení životního cyklu změn identit a schvalování změn. Funkční požadavky: - Zadávání požadavků uživatelů na změny v přiřazení rolí a skupin ke schválení nadřízeným - Možnost sledování stavu svých požadavků uživateli - E-mailové upozornění schvalovatele na požadavek ke schválení - Přehled úloh ke schválení pro každého schvalovatele - Schvalování či zamítnutí požadavků včetně uvedení zdůvodnění - Podporova vícekrokového schvalování - Podpora schvalování jedním nebo více schvalovateli (skupinou schvalovatelů) - Správce IDM může pracovat se všemi úlohami - Možnost větvení pro ošetření výjimek vzniklých při schvalování - Řešení zastupitelnosti - Eskalace - upozornění při překročení termínu splnění - Možnost vkládání systémových kroků s voláním webových služeb a spuštěním skriptů	Kapitola 6.1 Technické řešení
	Workflow - sledování	Průběh workflow bude možné sledovat v grafické podobě ve formě diagramu, ve kterém bude zřejmý stav probíhajícího workflow. Diagram bude ve obvyklém formátu pro zobrazní workflow např. aktivity diagram, BPMN nebo Archimate	Průběh workflow bude možné sledovat v grafické podobě ve formě diagramu, ve kterém bude zřejmý stav probíhajícího workflow. Diagram bude ve obvyklém formátu pro zobrazní workflow aktivity diagram, BPMN nebo Archimate	Kapitola 6.1 Technické řešení
	Upozornění	IDM zajistí zasílání konfigurovatelných emailových upozornění min. pro následující události: vytvoření a změna identity, referenčního objektu (systematizované místo, organizační jednotka, skupina, agenda, agendová činnostní role, aplikace, skupina aplikací, aplikační role atd.), problém při synchronizaci, vypršení hesla v Active Directory, vypršení platnosti certifikátu.	IDM zajistí zasílání konfigurovatelných emailových upozornění pro následující události: vytvoření a změna identity, referenčního objektu (systematizované místo, organizační jednotka, skupina, agenda, agendová činnostní role, aplikace, skupina aplikací, aplikační role) problém při synchronizaci, vypršení hesla v Active Directory, vypršení platnosti certifikátu.	Kapitola 6.1 Technické řešení
	Včasná upozornění	Upozornění na vypršení časových termínů musí být možno zasílat v předstihu. Velikost předstihu (např. 10 dnů) musí být možno konfigurovat pro každý typ upozornění samostatně.	Upozornění na vypršení časových termínů musí být možno zasílat v předstihu. Velikost předstihu je možno konfigurovat pro každý typ upozornění samostatně.	Kapitola 6.1 Technické řešení

Komodita K3 - Správa identit				
	Šablony upozornění	Šablony upozornění umožní definovat příjemce, předmět a obsah upozornění. U upozornění vázaného k identitám musí být možné nastavovat různé příjemce pro různé části organizační struktury (např. odbor, oddělení) apod. Šablony musí umožnit vložit do obsahu upozornění libovolný atribut identity a/nebo referenčního objektu.	Šablony upozornění umožní definovat příjemce, předmět a obsah upozornění. U upozornění vázaného k identitám bude možné nastavovat různé příjemce pro různé části organizační struktury (odbor, oddělení). Šablony musí umožnit vložit do obsahu upozornění libovolný atribut identity a/nebo referenčního objektu.	Kapitola 6.1 Technické řešení
	Kontext upozornění	Pro zasílání jednotlivých typů upozornění bude možno konfigurovat kontext, resp. podmínky, za jakých bude upozornění zasláno. V konfiguraci bude možné využít atributů identit a referenčních objektů. Příklad: notifikace budou generovány pouze pro identity v konkrétních uvedených skupinách, které mají uvedenu konkrétní aplikační role a konkrétní atribut atd.	Pro zasílání jednotlivých typů upozornění bude možno konfigurovat kontext, resp. podmínky, za jakých bude upozornění zasláno. V konfiguraci bude možné využít atributů identit a referenčních objektů. Příklad: notifikace budou generovány pouze pro identity v konkrétních uvedených skupinách, které mají uvedenu konkrétní aplikační role a konkrétní atribut.	Kapitola 6.1 Technické řešení
	Logování	Veškeré změny vyvolané požadavky uživatele a administrátorů/správců IDM budou provedeny transakčně. Budou logovány tak, aby bylo možné zpětně prokázat co, kdo a kdy měnil v identitách a referenčních objektech i v administraci a konfiguraci IDM. Záznam v logu bude obsahovat původní i novou hodnotu.	Veškeré změny vyvolané požadavky uživatele a administrátorů/správců IDM budou provedeny transakčně. Budou logovány tak, aby bylo možné zpětně prokázat co, kdo a kdy měnil v identitách a referenčních objektech i v administraci a konfiguraci IDM. Záznam v logu bude obsahovat původní i novou hodnotu.	Kapitola 6.1 Technické řešení
	Důvěryhodnot logování	Veškeré požadavky na změny v IDM bude možné zadávat výhradně prostřednictvím Portálu. Není přípustné realizovat požadavky ručními změnami textových soubory jako XML, CSV, atd. z důvodu zajištění zajištění úplného logování všech změn jednotlivých konfigurovaných parametrů IDM.	Veškeré požadavky na změny v IDM bude možné zadávat výhradně prostřednictvím Portálu. Není přípustné realizovat požadavky ručními změnami textových soubory jako XML, CSV z důvodu zajištění zajištění úplného logování všech změn jednotlivých konfigurovaných parametrů IDM.	Kapitola 6.1 Technické řešení
	Auditní report	IDM umožní export auditního reportu z údajů o identitách uložených v IDM a to i historických. Auditní reporty budou minimálně ve formátu XML nebo CSV a budou obsahovat souhrnné zobrazení daných uživatelů (identit) a jejich rolí v IS napojených na IDM, agendových rolí, přiřazených skupin ve vybraném časovém okamžiku od aktuálního času do minulosti.	IDM umožní export auditního reportu z údajů o identitách uložených v IDM a to i historických. Auditní reporty budou ve formátu XML nebo CSV a budou obsahovat souhrnné zobrazení daných uživatelů (identit) a jejich rolí v IS napojených na IDM, agendových rolí, přiřazených skupin ve vybraném časovém okamžiku od aktuálního času do minulosti.	Kapitola 6.1 Technické řešení
	Auditní report - výběr	Identity pro generování auditního reporty musí být možné vybrat (filtrovat) dle libovolných atributů identity včetně přidružených referenčních objektů.	Identity pro generování auditního reporty musí být možné vybrat (filtrovat) dle libovolných atributů identity včetně přidružených referenčních objektů.	Kapitola 6.1 Technické řešení
	Report RPP	Vestavěný report pro ohlašování působnosti v Registru práv a povinností. Bude obsahovat aktuální počty úředníků na agendových rolích a možnost porovnání s počtem úředníků k vybranému, dříve vygenerovanému, reportu. Report bude exportovatelný do CSV souboru.	Vestavěný report pro ohlašování působnosti v Registru práv a povinností. Bude obsahovat aktuální počty úředníků na agendových rolích a možnost porovnání s počtem úředníků k vybranému, dříve vygenerovanému, reportu. Report bude exportovatelný do CSV souboru.	Kapitola 6.1 Technické řešení
	Reporty uživatelů	Vestavěné reporty obsahující uživatele s přímo přiřazenými aplikačními rolemi a s aplikačními rolemi delegovanými od jiných uživatelů. Reporty budou exportovatelný do CSV souboru.	Vestavěné reporty obsahující uživatele s přímo přiřazenými aplikačními rolemi a s aplikačními rolemi delegovanými od jiných uživatelů. Reporty budou exportovatelný do CSV souboru.	Kapitola 6.1 Technické řešení

Komodita K3 - Správa identit				
	Reporty - zasílání	Reporty bude možné zasílat automaticky e-mailem na základě konfigurovatelných pravidel.	Reporty bude možné zasílat automaticky e-mailem na základě konfigurovatelných pravidel.	Kapitola 6.1 Technické řešení
	Reporty - historie	Automatické ukládání vygenerovaných reportů s možností pozdějšího zobrazení či stažení.	Automatické ukládání vygenerovaných reportů s možností pozdějšího zobrazení či stažení.	Kapitola 6.1 Technické řešení
	Reporty - porovnání	Snadné porovnání změn mezi vygenerovanými reporty stejného typu v prostředí Portálu.	Snadné porovnání změn mezi vygenerovanými reporty stejného typu v prostředí Portálu.	Kapitola 6.1 Technické řešení
	Webové služby (WS)	IDM bude poskytovat rozhraní webových služeb pro napojení dalších systémů s možností konfigurace v Portálu.	IDM bude poskytovat rozhraní webových služeb pro napojení dalších systémů s možností konfigurace v Portálu.	Kapitola 6.1 Technické řešení
	Standardy WS	Webové služby IDM budou definované v rozšířeném standardu WSDL a podporovat protokol SOAP.	Webové služby IDM budou definované v rozšířeném standardu WSDL a podporovat protokol SOAP.	Kapitola 6.1 Technické řešení
	Bezpečnost WS	Konfigurace webových služeb umožní konfigurovat přístup pro volání jednotlivých vybraných služeb pro každý odpovídající systémový účet samostatně.	Konfigurace webových služeb umožní konfigurovat přístup pro volání jednotlivých vybraných služeb pro každý odpovídající systémový účet samostatně.	Kapitola 6.1 Technické řešení
	Logování WS	Volání webových služeb bude logováno a bude možné je zobrazit v prostředí Portálu	Volání webových služeb bude logováno a bude možné je zobrazit v prostředí Portálu	Kapitola 6.1 Technické řešení
	Služby rozhraní WS	Rozhraní bude poskytovat minimálně následující služby: - Získání organizační struktury - Získání hierarchie systematizovaných míst - Získání seznamu identit - Získání nadřízené osoby pro daného zaměstnance - Získání seznamu aplikační rolí - Získání seznamu uživatelů dané aplikace - Získání seznamu agend a agendových rolí přiřazených dané aplikaci - Zápis seznamu aplikačních rolí do IDM - Zápis certifikátů do IDM - Zápis a změna identit	Rozhraní bude poskytovat minimálně následující služby: - Získání organizační struktury - Získání hierarchie systematizovaných míst - Získání seznamu identit - Získání nadřízené osoby pro daného zaměstnance - Získání seznamu aplikační rolí - Získání seznamu uživatelů dané aplikace - Získání seznamu agend a agendových rolí přiřazených dané aplikaci - Zápis seznamu aplikačních rolí do IDM - Zápis certifikátů do IDM - Zápis a změna identit	Kapitola 6.1 Technické řešení
	Služby rozhraní WS pro ISZR	Služba pro autorizaci pro ISZR (Informační systém základních registrů) – služba ověří validnost volání služby ISZR. Služba dále ověří v IDM: - Zda je evidován uživatel v IDM, který je součástí požadavku na ISZR - Zda je evidována aplikace v IDM, která je součástí požadavku na ISZR - Zda má tento uživatel v IDM nastaven přístup do aplikace, která je součástí požadavku na ISZR - Zda existuje v IDM v rámci evidence organizační struktury také evidence pro dané OVM, které je uvedeno v požadavku na ISZR	Služba pro autorizaci pro ISZR (Informační systém základních registrů) – služba ověří validnost volání služby ISZR. Služba dále ověří v IDM: - Zda je evidován uživatel v IDM, který je součástí požadavku na ISZR - Zda je evidována aplikace v IDM, která je součástí požadavku na ISZR - Zda má tento uživatel v IDM nastaven přístup do aplikace, která je součástí požadavku na ISZR - Zda existuje v IDM v rámci evidence organizační struktury také evidence pro dané OVM, které je uvedeno v požadavku na ISZR	Kapitola 6.1 Technické řešení

Komodita K3 - Správa identit				
		- Zda má aplikace, která je součástí požadavku na IZSR, v IDM povolenu agendovou činnostní roli a agendu, které jsou rovněž uvedeny v požadavku na ISZR.	- Zda má aplikace, která je součástí požadavku na IZSR, v IDM povolenu agendovou činnostní roli a agendu, které jsou rovněž uvedeny v požadavku na ISZR.	
	Synchronizace	Ruční i automatické spuštění synchronizací s propojenými systémy.	Ruční i automatické spuštění synchronizací s propojenými systémy.	Kapitola 6.1 Technické řešení
	Synchronizace - simulace	Spuštění synchronizací i v simulačním režimu pro ověření dopadu reálného spuštění bez ovlivnění produkčních dat a napojených systémů. Simulační logy budou zobrazitelné v Portálu.	Spuštění synchronizací i v simulačním režimu pro ověření dopadu reálného spuštění bez ovlivnění produkčních dat a napojených systémů. Simulační logy budou zobrazitelné v Portálu.	Kapitola 6.1 Technické řešení
	Simulace - průběh	Zobrazení jednotlivých stavů průběhu synchronizace bude k dispozici v přehledné grafické podobě.	Zobrazení jednotlivých stavů průběhu synchronizace bude k dispozici v přehledné grafické podobě.	Kapitola 6.1 Technické řešení
	Synchronizace - režimy	Pro napojení na jednotlivé systémy a implementaci jejich synchronizací s IDM umožní IDM u každého systému využít více režimů synchronizací (za předpokladu podpory napojovaného systému): - Plná synchronizace – prochází všechny objekty v IDM a synchronizuje je s objekty daného systému - Změnová synchronizace – synchronizuje vždy jen změny od poslední spuštěné synchronizace. - Okamžitá synchronizace konkrétní identity na vyžádání – synchronizuje okamžitě pouze vybranou identitu. - Rekonciliační synchronizace – synchronizace vytvoří rekonciliační report pro porovnání změn mezi nastavením identit a jejich oprávnění pro daný systém v IDM vs. nastavení identit a oprávnění přímo v připojeném systému. - Simulační synchronizace – synchronizace vytvoří report očekávaných změn v napojeném systému pro provedení ostré synchronizace. Report změn bude evidován jako pohled nebo přehledná souhrnná tabulka. - Historie běhu synchronizací – jednotlivé běhy synchronizací budou zaznamenány v historii dostupné v Portálu. Historie plné synchronizace bude obsahovat odkazy na objekty, které byly synchronizovány a log, co bylo u těchto objektů změněno v synchronizovaném systému. V případě změnové synchronizace pak bude v historii dále informace o události, která změnovou synchronizaci vyvolala.	Pro napojení na jednotlivé systémy a implementaci jejich synchronizací s IDM umožní IDM u každého systému využít více režimů synchronizací (za předpokladu podpory napojovaného systému): - Plná synchronizace – prochází všechny objekty v IDM a synchronizuje je s objekty daného systému - Změnová synchronizace – synchronizuje vždy jen změny od poslední spuštěné synchronizace. - Okamžitá synchronizace konkrétní identity na vyžádání – synchronizuje okamžitě pouze vybranou identitu. - Rekonciliační synchronizace – synchronizace vytvoří rekonciliační report pro porovnání změn mezi nastavením identit a jejich oprávnění pro daný systém v IDM vs. nastavení identit a oprávnění přímo v připojeném systému. - Simulační synchronizace – synchronizace vytvoří report očekávaných změn v napojeném systému pro provedení ostré synchronizace. Report změn bude evidován jako pohled nebo přehledná souhrnná tabulka. - Historie běhu synchronizací – jednotlivé běhy synchronizací budou zaznamenány v historii dostupné v Portálu. Historie plné synchronizace bude obsahovat odkazy na objekty, které byly synchronizovány a log, co bylo u těchto objektů změněno v synchronizovaném systému. V případě změnové synchronizace pak bude v historii dále informace o události, která změnovou synchronizaci vyvolala.	Kapitola 6.1 Technické řešení
	Synchronizace - správa	Vestavěná správa jednotlivých synchronizací včetně nastavení připojení na synchronizované systémy, nastavení plné a změnové synchronizace, počet změn, které je možné zpracovat, nastavení časového intervalu spouštění, nastavení intervalu odstávky. U jednotlivých synchronizací je rovněž požadováno,	Vestavěná správa jednotlivých synchronizací včetně nastavení připojení na synchronizované systémy, nastavení plné a změnové synchronizace, počet změn, které je možné zpracovat, nastavení časového intervalu spouštění, nastavení intervalu odstávky. U jednotlivých synchronizací je rovněž požadováno, aby bylo	Kapitola 6.1 Technické řešení

Komodita K3 - Správa identit				
		aby bylo možné vybírat organizace, které se mají z IDM synchronizovat s danými systémy. Správa bude součástí Portálu.	možné vybírat organizace, které se mají z IDM synchronizovat s danými systémy. Správa bude součástí Portálu.	
	Obecné konektory	Vestavěné obecné konektory pro správu identit v napojených systémech: - konektor pro spouštění CMD příkazů - konektor pro práci s CSV soubory - konektor pro práci s databází Microsoft SQL - konektor pro napojení na SOAP webové služby - konektor pro napojení na REST webové služby - konektor pro napojení na LDAP server s podporou LDAP v3	Vestavěné obecné konektory pro správu identit v napojených systémech: - konektor pro spouštění CMD příkazů - konektor pro práci s CSV soubory - konektor pro práci s databází Microsoft SQL - konektor pro napojení na SOAP webové služby - konektor pro napojení na REST webové služby - konektor pro napojení na LDAP server s podporou LDAP v3	Kapitola 6.1 Technické řešení
	Aplikační konektory	IDM bude spravovat identity a řídit oprávnění v dále vyjmenovaných systémech. V těchto systémech bude IDM vytvářet, aktualizovat, vytvářet uživatele a nastavovat jim oprávnění k rolím. - Microsoft Active Directory - Informační systém Ginis (GORDIC spol. s r.o.) - Microsoft Exchange, včetně vytváření schránek uživatelům - elektronická spisová služba AthenA vč. modulu iUsnesení (PilsCom, s.r.o.)	IDM bude spravovat identity a řídit oprávnění v dále vyjmenovaných systémech. V těchto systémech bude IDM vytvářet, aktualizovat, vytvářet uživatele a nastavovat jim oprávnění k rolím. - Microsoft Active Directory - Informační systém Ginis (GORDIC spol. s r.o.) - Microsoft Exchange, včetně vytváření schránek uživatelům - elektronická spisová služba AthenA vč. modulu iUsnesení (PilsCom, s.r.o.)	Kapitola 6.1 Technické řešení
	Konektory pro centrální systémy - RPP	IDM bude obsahovat evidenci matice práv a rolí dle Informačního systému základních registrů (ISZR-RPP - matice RPP) s následujícími funkcemi: - vedoucí pracovníci mohou zadávat k jednotlivým činnostem konkrétní uživatele (systemizovaná místa) - přidělování/odebírání agend/činností zaměstnancům vedoucími zaměstnanci s vazbou na systemizovaná místa - udržování a poskytování přehledu o oznámených působnostech, jejich stavech, kontrole přeregistrace a změnách - evidence přehledu legislativy včetně vazby na jednotlivé činnosti/agendy	IDM bude obsahovat evidenci matice práv a rolí dle Informačního systému základních registrů (ISZR-RPP - matice RPP) s následujícími funkcemi: - vedoucí pracovníci mohou zadávat k jednotlivým činnostem konkrétní uživatele (systemizovaná místa) - přidělování/odebírání agend/činností zaměstnancům vedoucími zaměstnanci s vazbou na systemizovaná místa - udržování a poskytování přehledu o oznámených působnostech, jejich stavech, kontrole přeregistrace a změnách - evidence přehledu legislativy včetně vazby na jednotlivé činnosti/agendy	Kapitola 6.1 Technické řešení
	Napojení na centrální systémy - JIP	IDM bude obsahovat správu identit, rolí a systémů evidovaných v systému JIP (Jednotní identitní prostor) s následujícími funkcemi: - Obousměrná synchronizace s JIP. - Automatické pravidelné načítání aplikací a rolí z JIP do IDM. - Automatické předávání identity včetně vazby na jednotlivé aplikační a agendové činnostní role z IDM do JIP. - Možnost změny hesla uživatele v JIP prostřednictvím Portálu.	IDM bude obsahovat správu identit, rolí a systémů evidovaných v systému JIP (Jednotní identitní prostor) s následujícími funkcemi: - Obousměrná synchronizace s JIP. - Automatické pravidelné načítání aplikací a rolí z JIP do IDM. - Automatické předávání identity včetně vazby na jednotlivé aplikační a agendové činnostní role z IDM do JIP. - Možnost změny hesla uživatele v JIP prostřednictvím Portálu.	Kapitola 6.1 Technické řešení

Komodita K3 - Správa identit				
	Zdrojový systém	IDM bude napojeno na personální systém FluxPaM (FLUX, spol. s r.o.). Z personálního systému budou načítány údaje o organizační struktuře, hierarchii pracovních míst, osobách a tyto údaje budou pro IDM sloužit jako zdrojové	IDM bude napojeno na personální systém FluxPaM (FLUX, spol. s r.o.). Z personálního systému budou načítány údaje o organizační struktuře, hierarchii pracovních míst, osobách a tyto údaje budou pro IDM sloužit jako zdrojové	Kapitola 6.1 Technické řešení

Komodita K4 - Školení kybernetické bezpečnosti				
Část	**Parametr**	**Popis povinného parametru**	**Uchazeč popíše způsob naplnění tohoto povinného parametru včetně značkové specifikace nabízených dodávek**	**Uchazeč uvede odkaz na přiloženou část nabídky, kde je možné ověřit naplnění parametru**
Obsah školení	Legislativní rámec	Zákon č.181/2014 Sb., a informační bezpečnost v organizaci	Zákon č.181/2014 Sb., a informační bezpečnost v organizaci	Kapitola 6.1 Technické řešení
	GDPR	Základní seznámení s nařízením GDPR (General Data Protection Regulation) - Obecným nařízení o ochraně osobních údajů- viz např. https://www.uoou.cz/gdpr-a-roleuoou/d-23082	Základní seznámení s nařízením GDPR (General Data Protection Regulation) - Obecným nařízení o ochraně osobních údajů- viz např. https://www.uoou.cz/gdpr-a-roleuoou/d-23082	Kapitola 6.1 Technické řešení
	Škodlivý software	projevy, druhy, obrana, preventivní chování, praktická ukázka provádění kontroly antivirovým programem	projevy, druhy, obrana, preventivní chování, praktická ukázka provádění kontroly antivirovým programem	Kapitola 6.1 Technické řešení
	Elektronická komunikace s úřady	datová schránka — co to je, k čemu slouží, zřízení a práce s datovou schránkou, elektronický podpis — co to je, jak s ním pracovat, jeho výhody a nevýhody	datová schránka — co to je, k čemu slouží, zřízení a práce s datovou schránkou, elektronický podpis — co to je, jak s ním pracovat, jeho výhody a nevýhody	Kapitola 6.1 Technické řešení
	Data vs. informace	kategorizace (osobních) dat, zásady a povinnosti zpracování z pohledu zaměstnavatele a zaměstnance, šifrování, praktická ukázka šifrování dat	kategorizace (osobních) dat, zásady a povinnosti zpracování z pohledu zaměstnavatele a zaměstnance, šifrování, praktická ukázka šifrování dat	Kapitola 6.1 Technické řešení
	Ochrana dat	zálohování, archivace a mazání dat, praktická ukázka zálohování dat	zálohování, archivace a mazání dat, praktická ukázka zálohování dat	Kapitola 6.1 Technické řešení
	Přístup k síti	PIN / heslo a jeho uložení, správné heslo, zásada prázdného stolu	PIN / heslo a jeho uložení, správné heslo, zásada prázdného stolu	Kapitola 6.1 Technické řešení
	Web	Používání webu, HTTPS, chatování, Skype, Facebook, výhody a rizika sociálních sítí, praktické ukázky	Používání webu, HTTPS, chatování, Skype, Facebook, výhody a rizika sociálních sítí, praktické ukázky	Kapitola 6.1 Technické řešení
	Elektronická identita	ztráta identity se mě (ne)týká?	ztráta identity se mě (ne)týká?	Kapitola 6.1 Technické řešení
	Mobilita	Používání mobilních zařízení, používání veřejných sítí a WIFI	Používání mobilních zařízení, používání veřejných sítí a WIFI	Kapitola 6.1 Technické řešení
	Mailování bezpečně	co e-mailem nikdy neposílat, spamy, phishing, hoax, bezpečné přihlášení/odhlášení, zálohování e-mailů, phishing	co e-mailem nikdy neposílat, spamy, phishing, hoax, bezpečné přihlášení/odhlášení, zálohování e-mailů, phishing	Kapitola 6.1 Technické řešení
	Kyberšikana	co to je, jaké jsou její formy a jaká preventivní opatření	co to je, jaké jsou její formy a jaká preventivní opatření	Kapitola 6.1 Technické řešení
	Incidenty	bezpečnostní incidenty a události, hlášení v organizaci,	bezpečnostní incidenty a události, hlášení v organizaci,	Kapitola 6.1 Technické řešení
	Závěr	obecný bezpečnostní test	obecný bezpečnostní test	Kapitola 6.1 Technické řešení

6.8 Požadavky na architekturu technického řešení

(1) Architektura komodit bude navržena tak, aby vhodně využívala a doplňovala stávající prostředky TC.

6.9 Požadavky na rozhraní

(1) Veškeré nabízené aktivní hardwarové produkty budou disponovat rozhraním SNMP v2 pro management a vzdálenou správu.

6.10 Požadavky na kompatibilitu s ostatními systémy

(1) Veškeré softwarové komponenty nabízeného řešení budou provozovány ve virtuálním prostředí VMware vSphere a jsou pro běh v tomto prostředí výrobcem podporovány.
(2) LAN přepínače budou kompatibilní s provozovaným systémem HP Intelligent Management Center.
(3) Řešení komodity K3 Správa identit bude kompatibilní s řešením komodity K2 SIEM na úrovni sběru logů

6.11 Požadavky na typy klientů

(1) Webová rozhraní komodit K2 a K3 budou kompatibilní s prohlížeči Internet Explorer, Firefox a Chrome v aktuálních verzích.

6.12 Požadavky na bezpečnost informací

(1) Veškeré nástroje pro správu hardware budou umožňovat správu interních účtů (jméno a heslo) a/nebo napojení na Active Directory.
(2) Veškeré nástroje pro správu hardware musí umožňovat definici s minimálně 2 úrovněmi oprávnění – monitoring (pouze čtení), administrátor (plná správa).
(3) Veškeré nástroje pro správu hardware musí komunikovat se zařízeními šifrovanými protokoly (SSH) Také v případě vestavěných nástrojů (např. www rozhraní hardware) bude použita šifrovaná komunikace (HTTPS).

6.13 Implementační služby

6.13.1 Požadavky na předimplementační analýzu – společné pro komodity K1 – K3

(1) Před implementací řešení zpracuje uchazeč předimplementační analýzu, pro následující oblasti a pro oblasti specifické pro jednotlivé komodity

(a) detailní popis stávajícího stavu, identifikaci slabých míst a bezpečnostních rizik, včetně vazeb na HW a SW systémy TC.
(b) Způsob začlenění nabízených komodit do prostředí TC.
(c) Síťová infrastruktura ve vztahu k plánovanému využití.
(d) SAN infrastruktura ve vztahu k plánovanému využití.
(e) Virtualizační infrastruktura (serverová, disková) ve vztahu k plánovanému využití.
(f) Integrace nabízených softwarových systémů.
(g) Rekonfigurace stávajících systémů.
(h) Dopady implementace na dostupnost a funkčnost stávajících služeb.
(i) Posouzení dopadů na non-IT technologie (spotřeba energií, tepelný výkon).
(j) Požadované součinnosti zadavatele a jejich rozsah.
(k) Návrh opatření k odstranění neshod zjištěných v průběhu analýzy.

(2) Výstupem předimplementační analýzy bude písemná zpráva, která podléhá schválení zadavatelem.

6.13.2 Požadavky na zpracování prováděcí dokumentace – společné pro komodity K1 – K3

(1) Uchazeč před zahájením implementačních prací zpracuje prováděcí dokumentaci, která bude důsledně vycházet z předimplementační analýzy a bude zahrnovat všechny aktivity potřebné pro řádné zajištění implementace předmětu plnění do stávajícího prostředí technologického centra.

(2) Prováděcí dokumentace bude před zahájením prací schválena zadavatelem.

(3) Prováděcí dokumentace bude zohleňovat podmínky stávajícího stavu, požadavky cílového stavu a musí obsahovat tyto části:

(a) Detailní popis cílového stavu včetně funkcionalit jednotlivých částí systému,
(b) Nutné a doporučené optimalizační a konfigurační změny dodávaných systému i všech navázaných systémů TC ORP (vSphere, LAN, SAN, zálohování, monitorování),
(c) Způsob zajištění potřebného HW a SW,
(d) Způsob zajištění koordinace realizace předmětu plnění s běžným provozem,
(e) Detailní návrh a popis postupu implementace předmětu plnění,
(f) Detailní popis zajištění bezpečnosti informací,
(g) Detailní harmonogram realizace včetně uvedení kritických milníků,
(h) Návrh designu síťového a bezpečnostního řešení a jeho konfigurace,
(i) Návrh designu aplikačních řešení,
(j) Vazby na stávající systémy a jejich konfigurace,
(k) Návrh akceptačních kritérií a akceptačních testů.

6.13.3 Požadavky na zajištění projektového vedení

(1) Uchazeč zajistí projektové vedení po celou dobu realizace zakázky certifikovaným specialistu.

(2) harmonogramu plnění – zde jsou uvedeny maximální možné lhůty pro jednotlivé kritické milníky. Údaj D značí datum podpisu smlouvy o dílo. Čísla značí počet kalendářních dnů.

Č.	Etapa projektu – činnost	Zahájení etapy	Ukončení etapy
1	Předimplementační analýza a zhotovení Prováděcí dokumentace	D	D+20
2	Předání Prováděcí dokumentace Zadavateli, připomínkové řízení	D+20	D+30
3	Zapracování připomínek a předání finální verze Prováděcí dokumentace – akceptace Zadavatelem	D+30	D+40
4	Dodávky a implementace	D+40	D+120
5	Školení kybernetické bezpečnosti	D+40	D+150
6	Školení administrátorů	D+90	D+120
7	Zkušební provoz	D+90	D+130
8	Akceptační testy	D+100	D+140
9	Zahájení plného provozu	D+150	-
10	Provedení opakovaných phishingových testů a případné opětovné absolvování webinářů	D+200	D+300

6.13.4 Požadavky na školení

(1) Uchazeč zajistí školení pracovníků zadavatele – administrátorů – na zařízení a systémy, dodávané v rámci této veřejné zakázky, a to v rozsahu předávané provozní dokumentace.
(2) Školení zajistí seznámení pracovníků zadavatele se všemi podstatnými částmi díla v rozsahu potřebném pro provoz, údržbu a identifikaci nestandardních stavů systému a jejich příčin.
(3) Rozsah školení je 24 hodin.
(4) Školení bude probíhat v sídle zadavatele.
(5) Předpokládá se účast max. 4 administrátorů.

6.13.5 Požadavky na provedení akceptačních testů, zkušební provoz a přechod do ostrého provozu

(1) Uchazeč navrhne způsob a provedení akceptačních testů.
(2) Součástí akceptačních testů musí být pro každou komoditu minimálně:
  (a) Prokázání kompletnosti dodávky a splnění povinných i hodnocených požadavků.
  (b) Prokázání vysoké dostupnosti u řešení, která jsou takto koncipována.
  (c) Prokázání aktivací software i hardware aktivačními klíči či jinými prostředky, je-li aktivace potřebná.
(3) Pro každou komoditu navrhne uchazeč vhodné doplňující testy a kritéria, kterými bude prokázána bezproblémová funkčnost a odpovídající výkon a stabilita dodaného řešení.
(4) O provedení akceptace a jejím výsledku bude vyhotoven písemný protokol.
(5) Uchazeč zajistí zkušební provoz v délce 20 dnů včetně technické podpory 1 specialisty na dodané řešení s dojezdem maximálně do 2 hodin od nahlášení požadavku v pracovní den v době od 8h do 17h.
(6) Přechodem do ostrého provozu se rozumí okamžik úspěšné akceptace díla včetně vypořádání všech vad a nedodělků.

6.13.6 Záruky a servisní podmínky

(1) Zadavatel požaduje záruku na veškeré dodané služby v délce trvání 3 měsíců a zařízení 24 měsíců (není-li u konkrétní komodity uvedeno jinak) od okamžiku ukončení implementace a předání do produkčního provozu.
(2) Není-li u konkrétní komodity uvedeno jinak, je provedení záruční opravy do 5-ti pracovních dnů nebo poskytnutí náhradního prvku shodných nebo lepších parametrů po dobu opravy.
(3) Veškeré opravy po dobu záruky budou bez dalších nákladů pro provozovatele.
(4) Uchazeč ve své nabídce výslovně uvede všechny podmínky záruk.
(5) Bezplatný přístup k aktualizacím software a firmware dodaných komodit minimálně po dobu záruky.
(6) Veškeré opravy po dobu záruky budou provedeny bez dalších nákladů pro zadavatele.
(7) Veškeré komponenty, náhradní díly a práce, poskytnuté v rámci záruky budou poskytnuty bezplatně.

(8) Součástí technické podpory bude spolupráce s administrátory zadavatele při řešení nekompatibilit aplikací a systémů.
(9) Pro hlášení servisní požadavků zajistí uchazeč Zhotoviteli přístup ke svému helpdeskovému systém s on-line přístupem pro kompletní správu požadavků včetně uchování historie požadavků a jejich řešení. Detailní popis helpdeskového systému a jeho obsluhy je v příloze č.3 nabídky. Provozní doba helpdeskového systému je 7-17 hod. v pracovních dnech.

6.14 Požadavky na zabezpečení provozu

Návrh podmínek podpory zajištění provozu, zajišťující garantovanou úroveň služeb podpory zajištění provozu předmětu plnění a také stávajících technologií TC ORP od doby předání do plného provozu.

6.14.1 Definice

(1) **24x7** – služba nebo zařízení je v provozu/dostupné 24 hodin a 7 dní v týdnu s garancí minimálně 95% dostupnosti
(2) **9x5** - služba nebo zařízení je v provozu/dostupné 9 hodin denně v běžnou pracovní dobu po všechny pracovní dni v týdnu s garancí minimálně 95% dostupnosti
(3) **BD** – Business Day – standartní pracovní den
(4) **BE (Best Effort)** - uchazeč vyvine maximální možné úsilí na provedení požadavku a zejména na zajištění požadovaných parametrů Prvku IT v nejkratší možné době.
(5) **Běžná pracovní doba** – čas mezi 8:00 a 17:00 v Pracovní dny.
(6) **Člověkohodina** - práce Pracovníka uchazeče v rozsahu jedné (1) hodiny v rámci Pracovního dne.
(7) **Člověkoden** - práce Pracovníka uchazeče v rozsahu jednoho (1) Pracovního dne.
(8) **Doba odezvy (Response time – R)** – metrika definující čas, který uplyne od nahlášení Požadavku na Servisní službu do začátku provádění Servisní služby. Do Doby odezvy se započítává pouze čas, určený Servisním kalendářem k řešení daného Požadavku. Za odezvu se považuje jakákoliv prokazatelná reakce servisního pracovníka Dodavatele směřující k odstranění incidentu, zodpovězení Dotazu nebo přípravy Nového požadavku.
(9) **Dotaz –** funkce v systému existuje, Prvek IT pracuje v souladu s Prováděcí dokumentací, ale pověřená osoba zákazníka s ní není dostatečně seznámena a podá Požadavek - Dotaz na Hot-line nebo HelpDesk
(10) **HelpDesk** – nepřetržitě dostupný automatizovaný systém pro vzdálené zadávání a správu požadavků,
(11) **Hot-line** –pracoviště uchazeče přijímající Požadavky od zadavatele na definovaných telefonních číslech nebo elektronických komunikačních kanálech.
(12) **Incident**- událost způsobující odchylku od očekávané funkce Prvku IT, která způsobuje nebo může způsobit přerušení anebo snížení kvality této funkce.
(13) **Priorita incidentu** - závažnost incidentu dle klasifikace Kontaktní osoby zadavatele.
(14) **Koncová zařízení** - počítače uživatelů, jejich programové vybavení a periferní zařízení k počítačům připojená (např. tiskárny, skenery).
(15) **Monitorování** - sledování prvků IT prostředky Vzdáleného přístupu, zda jsou funkční. Sledování, zda provozní charakteristiky prvků IT nepřesahují stanovené hodnoty, eventuálně neklesají pod stanovené hodnoty. Monitorováním se případně rozumí sledování a archivování jejich provozních charakteristik.
(16) **Proaktivní monitorování**-monitorování prováděné dle charakteru provozu a činnosti Prvku IT v režimu 24x7 (komunikační infrastruktura) nebo v režimu 9x5 (technologické centrum).
(17) **Náhradní zařízení** – zařízení podobných vlastností (parametrů).
(18) **Požadavek** - žádost o provedení Servisní služby na jednom nebo více Prvcích IT.
Požadavek může zahrnovat:
(a) žádost o odstranění závady (nefunkční Prvek IT nebo nesprávná činnost Prvku IT) - incidentu
(b) žádost o poskytnutí konzultace
(c) žádost o provedení Změny
Požadavek může:
(d) být zadán zadavatelem jako jednorázový
(e) být zadán zadavatelem jako opakující se činnost
(f) vzniknout jako výstup Monitorování

(g) vzniknout na základě Správy a údržby Prvku IT

(19) **NBD-Next Business Day** – následující pracovní den

(20) **Neprodleně** – bez zbytečného odkladu, s vyvinutím maximálního úsilí na zjednání nápravy nebo zajištění činnosti, nejpozději však následující Pracovní den.

(21) **Pracovní dny** - všechny dny, kromě sobot a nedělí nebo zákonem stanovených svátků a dnů pracovního klidu, během nichž dohodnuté pracovní činnosti budou prováděny v čase od 8:00 do 17:00 hodin.

(22) **Prvek IT** - zařízení (Koncové zařízení, server či jiný hardware), program (software) nebo komunikační linka.

(23) **Rozsah poskytovaných služeb** – specifikace Služby a kvantifikace rozsahu Služby

(24) **Řešitel** - Pracovník uchazeče, podílející se na řešení Požadavku.

(25) **Report** – přehledový dokument, ve kterém je popsán průběh realizace Plnění za uplynulé období a hodnoty sledovaných parametrů.

(26) **SLA (Service Level Agreement)** - definice kvalitativních parametrů/metrik Služby

(27) **Správa a údržba** - provádění činností, které jsou nutné ke správné a bezchybné funkci Prvku IT. Zpravidla se jedná o pravidelnou kontrolu stavu prvků IT a provádění takových Změn, které se pravidelně opakují, nebo jsou provedeny na základě kontroly stavu Prvku IT.

(28) **Služby** – činnosti potřebné pro řádné zabezpečení podpory provozu díla

(29) **Úplné odstranění závady** - se rozumí dosažení stavu, který byl akceptován v rámci smlouvy o dílo nebo je popsán v Prováděcí dokumentaci popř. v dokumentaci Prvku IT.

(30) **Vzdálená správa** – provádění činností na Prvcích IT, přičemž činnosti nejsou prováděny v místě provozovny zadavatele, ale prostřednictvím Vzdáleného přístupu z místa provozovny uchazeče.

(31) **Vzdálený přístup** – připojení z provozovny uchazeče k zařízení zadavatele pomocí komunikační linky, na které je vytvořeno dočasné nebo trvalé spojení.

(32) **Zprovoznění náhradním způsobem** - se rozumí zajištění základních funkcí systému, tedy dosažení stavu, kdy není vážně omezena funkčnost informačního systému nebo jeho částí.

(33) **Změna** - změna parametrů Prvku IT nebo instalace, přemístění či odinstalace Prvku IT.

(34) **Legislativní servis** - legislativním servisem se rozumí úprava stávající funkčnosti stávajícího systému (software), kterou je nutné provést, protože stávající funkcionalita by nutila zákazníka konat v rozporu s novou legislativní úpravou. Legislativní úpravou v žádném případě není doplnění funkcionality (řešené oblasti), kterou stávající systém (software) nepokrýval.

(35) **Reklamace** - reklamací je požadavek vznesený na přezkoumání a odstranění vlastnosti Prvku IT v čase záruční doby, která je v rozporu:

(a) se standardní funkčností Prvku IT a tento rozpor je vůči uživatelské dokumentaci produktu,

(b) s funkcionalitou definovanou ve smlouvě (jejích přílohách), případně akceptačním protokolu funkcionality Prvku IT,

(c) s platnou legislativou ČR k datu podání požadavku.

(36) **Konfigurační management** - jde o službu poskytovanou za účelem udržení aktuální technické dokumentace. V případě jakékoliv provedené změny, bude aktualizována provozní dokumentace o konfiguraci systému včetně zaznamenaných změn. Dokumentace je uložena u uchazeče i zadavatele. Poskytuje informace o Prvcích IT a službách včetně informací o aktuálních verzích. Zahrnuje rovněž správu veškeré dokumentace ke všem prvkům infrastruktury a služeb. Obvykle je využíván automatizovaný nástroj pro sběr a aktualizaci většiny údajů v konfigurační databázi.

(37) **Patch Management** - jedná se o preventivní činnost týkající se především operačních systémů a instalace opravných balíčků, kde hlavním cílem je udržet systém v aktuálním stavu a s nainstalovanými aktuálními softwarovými komponentami.

(38) **Hotline podpora** - jde o službu zajišťující poradenství po telefonu nebo elektronické komunikaci

(39) **Maintenance** – jedná se o zajištění nových a opravných verzí software (včetně hlavních verzí), nových verzí firmware, přístupu k technické podpoře výrobce a přístupu k databázi řešených problémů.

(40) **Monitorování** – jedná se o službu nepřetržitého online monitorování systémů s upozorněním na kritické nebo neobvyklé události, upozornění budou automaticky zasílána oprávněným pracovníkům zadavatele. Součástí služby je vzdálený přístup k aktuálním i historickým údajům o stavu systému. Monitorování je souborem takových opatření, která umožňují v kterémkoli čase znát stav Systému a Systémů třetích stran, minimálně v rozsahu:

(a) monitoring operačních systémů,

(b) monitoring sítě a síťových propojení Systému a Systémů třetích stran,

(c) monitoring databázových systémů,
(d) monitoring diskových úložišť,
(e) monitoring prvků IT třetích stran, které mohou ovlivňovat chod Systému, pokud jsou tyto Prvky IT součástí Dodávky nebo mohou mít na funkci a/nebo dostupnost Prvku IT negativní vliv způsobující incident kategorie A nebo B.

(41) **Profylaxe** - profylaxe zahrnuje aktualizace firmware zařízení, aktualizace administrátorských nástrojů, kontrolu logů, kontrolu vytížení a využití, kontrolu kapacit.

6.14.2 Specifikace rozsahu požadované podpory provozu

(1) Základní rozsah systémové podpory v rámci měsíčního paušálu:
(a) Pravidelné servisní prohlídky a revize předepsané výrobci
(b) Průběžné monitorování prvků IT pokrývaných touto smlouvou dalších popř. prvků IT, které mohou ovlivnit jejich chod. Počet sledovaných parametrů nesmí být prakticky omezen (min. stovky), administrátoři MMKV musí mít přístup ke sledovaným parametrům alespoň v režimu čtení.
(c) Provádění hardwarových oprav IT prvků pokrývaných v rámci smlouvy minimálně v kvalitě a parametrech jako po dobu záruky. Cena náhradních dílů je zahrnuta v paušální ceně.
(d) Řešení Požadavků a incidentů – dle podmínek SLA
(e) Profylaxe - každých 6 měsíců
(f) Hotline podpora v režimu 9x5
(g) Patch management
(h) Odborná podpora v režimu 9x5 – vzdálené konzultace pro podporované služby/produkty.
(i) Celkový rozsah služeb Hotline a Odborné podpory v rámci měsíčního paušálu 8 hodin. Minimální dostupnost podpory v režimu 9x5.

(2) Další služby v rámci měsíčního paušálu
(a) Zajištění tj. dodávku, instalaci a zprovoznění maintenance a aktualizací (včetně bezpečnostních signatur apod.) pro veškerý dodaný software – min. 1x ročně a v případech vynucených změnou legislativy či změnou navázaného systému. Pro operační systém serveru jsou požadovány pouze aktualizace, nikoli nové verze.
(b) Zajištění tj. instalaci a zprovoznění maintenance (nových verzí firmware a ovládacího software a přístupu k technické podpoře výrobce) a aktualizací pro veškerý hardware dodaný v rámci této zakázky – min. 1x ročně
(c) Helpdeskový systém s on-line přístupem pro kompletní správu požadavků včetně uchování historie požadavků a jejich řešení.
(d) Rozšířený monitoring systému a zpracovávaných dat a specifické služby provozního zajištění komodity K2 SIEM a NBA v rozsahu potřebném pro provádění následujících služeb v režimu 9x5:
(i) Informování odpovědných osob zadavatele o vzniku bezpečnostního incidentu v reálném čase za pomocí základních komunikačních nástrojů (mail / SMS /tel)
(ii) Zahájení řešení bezpečnostního incidentu do 4hodin od vzniku, řízení souvisejících činností správců a případných dalších dotčených osob.
(iii) Zakládání tiketů, proaktivní komunikace o jejich řešení.
(iv) Komunikace s třetí stranou jako NBU, NCKB, CSIRT atd.
(v) Rozšířený reporting - detailní report o událostech a incidentech s návrhy systematických opatření 1x měsíčně. Vzdálená prezentace reportu např. formou videokonference.
(vi) Pravidelné skenování aktiv a zranitelností min. 1x týdně.

(3) Uchazeč zpracuje a poskytne zadavateli každý měsíc Report, ve kterém je popsán průběh realizace Plnění za uplynulé období, provedené služby a návrh doporučených opatření pro další období pro zvýšení bezpečnosti a dostupnosti TC ORP a prevenci incidentů.

6.14.3 Způsob poskytování plnění

(1) Plnění je poskytováno zejména následujícím způsobem:

(a) Prostřednictvím pracovníka uchazeče přímo na pracovišti zadavatele,
(b) Prostřednictvím pracovníka uchazeče Vzdálenou správou,
(c) Prostřednictvím pracovníka uchazeče formou vzdálené konzultace,
(d) Po dohodě smluvních stran automatizovanými nástroji při Monitorování, umožňují-li to technické prostředky na straně zadavatele.

(2) Uchazeč provede písemný záznam o provedení Služby na pracovišti zadavatele, který předá zadavateli a nechá si ho od něj potvrdit. Servisní služby, které jsou poskytovány vzdálenou formou, mohou být evidovány v elektronickém seznamu provedených úkonů.

(3) Zadavatel je povinen zabezpečit uchazeči podmínky pro řádné plnění, zejména
(a) v případě Monitorování a Vzdálené správy zajistit a udržovat podmínky pro Vzdálený přístup uchazeče k prvkům IT,
(b) zajistit dostupnost nebo odpovídající zástup Odpovědné osoby zadavatele, vyhrazení odpovídajících časových kapacit Odpovědné osoby zadavatele a zajištění efektivní součinnosti odborných pracovníků zadavatele,
(c) zajistit přístup k Provoznímu prostředí, který je nezbytný pro poskytování Služeb, včetně přístupu do prostor v objektu, kde je předmětný Prvek IT umístěn, případně přístup do prostor, v nichž jsou umístěna zařízení související s podporovaným systémem,
(d) zabezpečit přítomnost kvalifikované osoby, která poskytne pracovníku uchazeče veškeré informace či přístupy potřebné k podpoře předmětného systému, resp. informace o zařízeních a programovém vybavení souvisejícím s předmětným systémem,
(e) umožnit uchazeči v případě nutnosti a po předchozím oznámení odstavení technických prostředků z běžného provozu,
(f) zajistit součinnost třetí strany, jestliže je to pro provedení služby potřebné.

(4) V případě, že nebudou uvedené podmínky zadavatelem prokazatelně zabezpečeny, lhůta pro vyřešení případného incidentu se zastaví a počítat se bude až po obnovení zabezpečení uvedených podmínek.

(5) Uchazeč je v případě potřeby též z vlastní iniciativy oprávněn požádat zadavatele o dodatečné údaje o incidentu a o nezbytnou součinnost zadavatele na řešení incidentu, bez které nelze zahájit či pokračovat v řešení incidentu. Tím se zastavuje započítávání času, což je rozhodující pro určení čistého času řešení incidentu při hodnocení úrovně poskytovaných služeb (SLA).

(6) Zadavatel je povinen
(a) písemně či elektronicky potvrdit uchazeči provedení služby,
(b) zajistit zálohování dat i programů a výměnu zálohovacích médií dle zálohovacího plánu, jejich dostupnost v případě potřeba a jejich uložení na bezpečných místech tak, aby bylo nešlo k jejich ztrátě nebo poškození,
(c) poskytovat potřebné nebo vyžádané informace a podklady včetně dokumentace k předmětnému systému nebo zařízení a programovému vybavení, které s ním souvisí, nejpozději do tří (3) Pracovních dnů po jejich písemném či ústním vyžádání, pokud se o obě strany nedohodnou jinak.

6.14.4 Seznam prvků IT

Následující tabulka obsahuje seznam prvků IT, u niž je požadováno Zabezpečení provozu

Prvky IT				
Prvek	**Popis**	**Počet**	**Platná záruka**	**Poznámka**
Hardware				
1	Veškeré hardwarové prvky dodané v rámci této zakázky	x	dle nabídky	
Software				
2	Systém SIEM a NBA komodity K2	x	dle nabídky	
3	Systém pro správu identity komodity K3	x	dle nabídky	Platnost maintenence integrovaných systémů zajišťuje zadavatel na vlastní náklady mimo tuto zakázky, poskytne přístup uchazeči

6.14.5 Postup při řešení požadavků

(1) Zadavatel bude požadavek oznamovat uchazeči bez zbytečného odkladu jedním ze způsobů a na kontaktních místech uvedených ve Smlouvě o zabezpečení provozu, kam budou mít zajištěny přístup pověřené osoby zadavatele. Momentem nahlášení požadavku zadavatelem na hot-line nebo zadáním požadavku do HelpDesk začíná běžet lhůta pro Dobu odezvy.

(2) Součástí nahlášení požadavku zadavatelem musí být:

(a) navrhovaná kategorizace a závažnost,

(b) popis incidentu nebo Požadavku,

(c) jiné relevantní upřesňující informace, včetně případných textových či obrazových příloh,

(d) kontaktní osoba.

(3) Uchazečem používaný systém pro HelpDesk pokryje uvedené informace pro nahlášení požadavku.

(4) Incidenty budou před jejich nahlášením začleněny do skupin, viz dále a dle těchto skupin bude Uchazeč přistupovat k jejich řešení:

Incident/vada kategorie A
Prvek IT/služba není použitelná ve svých základních funkcích nebo se vyskytuje funkční závada znemožňující používání služby. Tento stav může ohrozit běžný provoz, případně může způsobit větší finanční nebo jiné škody.
Incident/vada kategorie B
Prvek IT/služba je ve svých funkcích degradována tak, že tento stav omezuje běžný provoz.
Incident/vada kategorie C
Ostatní - drobné incidenty/vady, které nespadají do kategorií A a/nebo B a které nejsou způsobeny software třetích stran.
Incident/vada kategorie D
Incidenty/vady, které jsou způsobeny software třetích stran.

(5) Uchazeč potvrdí obdržení požadavku dle podmínek SLA a bez ohledu na způsob nahlášení provede evidenci Požadavku v systému HelpDesk a poskytne zadavateli informace o předpokládaném způsobu řešení požadavku, požadavcích na součinnost zadavatele a předpokládaný termín vyřešení požadavku.

(6) Uchazeč v průběhu řešení požadavku, pokud mu to charakter požadavku a způsob řešení umožňuje, průběžně informuje zadavatele o aktuálním stavu a případných změnách v předpokládaném způsobu, požadované součinnosti a termínů vyřešení. V případě že uchazeč v průběhu řešení požadavku zjistí, že se jedná o incident, jehož zdroj je prvek třetích stran, informuje zadavatele o této skutečnosti, předpokládaném způsobu, požadované součinnosti a termínů vyřešení – zároveň přeřadí incident do kategorie D a pokračuje v řešení v režimu BE (Best Effort).

(7) Zjistí-li uchazeč v průběhu řešení incidentu, že incident je neodstranitelný, je v rámci Běžné pracovní doby povinen nepřetržitě pracovat na náhradním řešení a informovat o tomto stavu zadavatele. Výskyt neodstranitelného incidentu může být ze strany zadavatele považován za podstatné porušení této smlouvy v případech, že incident byl způsoben předchozím přímým jednáním uchazeče, pokud o nich mohl mít s vynaložením veškeré odborné péče povědomost.

(8) Zjistí–li uchazeč v průběhu řešení incidentu, že incident má přímou souvislost s neodborným či neoprávněným jednáním osob zadavatele případně byl incident vyvolán produkty či službami třetí osoby, je uchazeč povinen bezodkladně informovat o tomto stavu zadavatele. zadavatel se zavazuje bezodkladně uhradit v plné výši náklady nad rámec této smlouvy uchazečem prokazatelně vynaložené k řešení incidentu, přičemž samotná identifikace incidentu je součástí plnění této smlouvy.

(9) Zadavatel je oprávněn dořešení incidentu kdykoliv zastavit či pozastavit, přičemž nárok uchazeče na úhradu již vynaložených prostředků zůstává nedotčen. Incident je v tomto případě považován za vyřešený.

(10) V případě úspěšného vyřešení požadavku, je řešitel před ukončením požadavku povinen provést ověření funkčnosti služby (pokud je to možné). Iniciátora incidentu informuje o:

(a) čase vyřešení požadavku,

(b) v případě incidentu specifikuje příčinu (pokud je známa),

(c) vyzve iniciátora k ověření funkčnosti služby.

(11) Po ověření funkčnosti ze strany zadavatele se Požadavek považuje za vyřešený.

(12) Po vyřešení požadavku uchazeč požadavek uzavře v systému HelpDesk a informuje zadavatele. V případě incidentu kategorie A zasílá návrh opatření pro snížení nebo eliminaci možnosti opakování stejného incidentu.
(13) Zadavatel má právo ve lhůtě 10 dnů od uzavření požadavku vznést výhrady nebo připomínky ke způsobu řešení nebo k výslednému stavu Prvku IT; v takovém případě se požadavek nepovažuje za uzavřený a Strany se zavazují zahájit společné jednání za účelem odstranění veškerých vzájemných rozporů a nalezení shody nad ke způsobem řešení nebo výsledném stavu Prvku IT, a to nejpozději do pěti (5) pracovních dnů od výzvy kterékoliv Strany.

6.14.6 Podm+ínky SLA

(1) Uchazeč se zavazuje dodržovat při řešení požadavků následující parametry (SLA).

Kategorie incidentu	Garantovaná doba přijetí a akceptace hlášeného incidentu	Garantovaná doba zahájení prací na řešení incidentu po řádném nahlášení	Garantovaná doba ukončení incidentu po řádném nahlášení
A	15 min	1 hod	Nejpozději do 24 hod
B	15 min	4 hod	NBD
C	15 min	NBD	5BD
D	15 min	NBD	BE

(2) Pro předání požadavků na plnění závazků vyplývajících z SLA, je požadováno použití technologie umožňující nepřetržitý dálkový přístup v českém jazyce.
(3) V rámci vymezení předmětu SLA uchazeč nejlépe v technické příloze dostatečně přesně popíše, jaké služby a činnosti zadavatele jsou pro plnění SLA zcela zásadní a kritické, respektive na jakých aplikacích a službách je provoz systémů závislý. Dále uchazeč popíše, jakým způsobem zajistí dosažení podmínek SLA, možnosti měření SLA a možnosti ověření dosahování SLA, které bude mít zadavatel k dispozici.

Čestné prohlášení uchazeče o původu zboží

Uchazeč(i):

Název:	AutoCont CZ a.s.
Sídlo:	Hornopolní 3322/34, 702 00 Ostrava
IČ:	47676795
DIČ:	CZ47676795

Prohlašuji tímto, že veškeré produkty, které uchazeč dodává v rámci plnění Zadavateli, splňují následující podmínky:

(a) jsou nové, byly oprávněně uvedeny na trh v EU nebo pochází z autorizovaného prodejního kanálu výrobce,
(b) mají plnou záruku od výrobce,
(c) mohou být podporovány výrobcem a mohou být součástí servisního a podpůrného programu výrobce,
(d) obsahují všechny nezbytné licence na používání příslušného softwaru,
(e) jsou v databázi výrobce uvedeny jako prodaná kupujícímu,
(f) jsou určeny pro provoz v České republice.

Výjimkou mohou být pouze jednotlivé komponenty určené pro rozšíření stávajících technologií, které již výrobce nedodává (např. z důvodu náhrady novým modelem). V takovém případě lze nabídnout originální komponenty dodávané v rámci servisního programu a splňující požadované parametry včetně záruk.

V Karlových Varech dne 15.1.2018

[redacted]

Ing Zdeněk Chobot
na základě plné moci

7 Kalkulace nabídkové ceny

7.1 Předmět plnění - implementace

Položka	Ks/ sou-bor	Celková cena bez DPH	Částka DPH	Celková cena s DPH
K1 - Rozšíření kapacit Technologického centra ORP				
Virtualizační server	1	521 128 Kč	109 437 Kč	630 564 Kč
Licence operačního systému - sada	1	195 423 Kč	41 039 Kč	236 462 Kč
Síťové přepínače a sondy síťových toků	4	830 547 Kč	174 415 Kč	1 004 962 Kč
Kabely, optické moduly	1	130 282 Kč	27 359 Kč	157 641 Kč
Rozšíření kapacity síťového úložiště NAS pro archivaci SIEM	1	76 215 Kč	16 005 Kč	92 220 Kč
Rozšíření kapacit diskových polí pro SIEM	1	78 169 Kč	16 416 Kč	94 585 Kč
K2 - SIEM a NBA				
SIEM a NBA	1	1 179 403 Kč	247 675 Kč	1 427 078 Kč
K3 - Správa identit				
Systém pro správu identity (Identity management - IDM)	1	1 911 394 Kč	401 393 Kč	2 312 787 Kč
K4 - Školení kybernetické bezpečnosti				
Školení kybernetické bezpečnosti	1	734 134 Kč	154 168 Kč	888 302 Kč
Celková cena				
		5 656 695 Kč	**1 187 906 Kč**	**6 844 601 Kč**

7.2 Provozní podpora

Název služby	Cena bez DPH	DPH v zákonné výši v Kč	Cena včetně DPH v Kč
Zabezpečení podpory provozu	3 760 400 Kč	789 684 Kč	4 550 084 Kč
Rozšířená záruka HW	8 500 Kč	1 785 Kč	10 285 Kč
Maintenance SW	1 547 000 Kč	324 870 Kč	1 871 870 Kč
CELKEM	**5 315 900 Kč**	**1 116 339 Kč**	**6 432 239 Kč**

8 Přílohy

8.1 Příloha č.1 - Popis postupu implementace předmětu plnění

Obsah dokumentu

Obecné podmínky implementace

Následující podmínky vycházejí z obecných zásad řízení implementačních projektů a zahrnují zkušenosti uchazeče získané z velkého množství (stovky) projektů obdobného zaměření. Popis je použitými pojmy koncipován jako materiál nevyžadující formální vzdělání v oblasti projektového řízení a řízení IT služeb a orientuje se především na praktickou stránku a srozumitelnost implementačního postupu.

Řízení implementace

Z pohledu implementace bude uchazeč přistupovat k veřejné zakázce „Rekonstrukce terminálové farmy" jako k jednomu projektu složenému z více vzájemně provázaných částí – jednotlivých komodit. Výhodou toho přístupu pro zadavatele je jednotné řízení celého projektu jedním **projektovým manažerem**, který zajišťuje plnění smluvních a dalších sjednaných činností a koordinuje činnosti jednotlivých specialistů uchazeče a jeho subdodavatelů. Projektový manažer je tak hlavním komunikačním kontaktem pro zadavatele v oblasti organizace projektu – tímto způsobem jsou minimalizovány nároky na projektový tým zadavatele z pohledu komunikace a koordinace projektu. Projektový manažer dále zajišťuje dodržování časového harmonogramu, organizaci projektových a technických schůzek, pořizování a schvalování zápisů a pravidelný reporting o průběhu projektu – tyto činnosti tak probíhají v režii uchazeče a zadavatel jimi není zatěžován. Projektový manažer je správcem případných změnových požadavků navrhovaných uchazečem či zadavatelem. V případě potřeby je projektový manažer eskalačním kontaktem první úrovně.

Pro zajištění technické konzistence celého řešení a postupu bude v implementačním týmu ustanovena role **architekta řešení** – jde o technickou roli zastřešující odbornými znalostmi celou šíři implementovaného řešení a zajišťující optimální integraci (provázání) jednotlivých technologií a částí projektu (komodit) na technické úrovni. Architekt řešení je hlavním komunikačním kontaktem zadavatele v technických záležitostech - tímto způsobem jsou minimalizovány nároky na projektový tým zadavatele z pohledu komunikace a koordinace projektu v technických záležitostech.

Zajištění vysoké odbornosti implementace a přenosu know-how

Základní úroveň využití a uplatnění doporučených postupů výrobců bude zajištěna prováděním implementačních činností specialisty certifikovanými výrobci pro danou oblast implementace. Prokázání znalostí a pochopení implementačních postupů a pravidel spolu s prokázáním technických znalostí produktů a technologií je stěžejním cílem certifikačních procesů výrobců.

Vedle technických certifikací budou všichni specialisté uchazeče i jeho poddodavatelů disponovat praktickými zkušenostmi z implementací technicky i rozsahem obdobných projektů, které uplatní v analytické, návrhové i instalační fázi projektu. Zadavatel tak získá významnou přidanou hodnotu současně v několika oblastech:

- uplatnění osvědčených postupů a řešení z obdobných projektů (tzv. best practice)
- zkrácení všech fází projektu na minimum – eliminace nevhodných variant a postupů
- minimální zátěž projektového týmu zadavatele – předkládání konkrétních návrhů či malého počtu jasně vyhodnotitelných variant namísto dotazů

Zajištění bezpečnosti

Kromě smluvního zajištění důvěrnosti dat a informací a obvyklého dodržování bezpečnostních norem a pravidel bude uchazeč v průběhu implementace klást důraz na následující oblasti bezpečnosti:

- zajištění kontinuity provozu – vzhledem k prostředí vyžadujícímu trvalý provoz IT technologií bude implementační tým nasazovat nové technologie tak, aby byl v případě potřeby schopen rychle obnovit předchozí (tzv. poslední funkční) stav

- zajištění technické ochrany dat – vzhledem k rozsáhlosti projektu a počtu změn bude uchazeč průběžně provádět zálohy dat

Dodavatele bude respektovat provozní podmínky zadavatele a činnosti vyžadující omezení provozu bude provádět v předem sjednaných časech, ve kterých bude omezení provozu zadavatele minimální. Dodavatel bude preferovat technologické postupy a řešení, které v maximální možné míře eliminují omezení provozu zadavatele a případné součinnostní kroky uživatelů či administrátorů (např. při migracích dat) umožní rozložit v čase tak, aby jejich vykonáváním nebyl omezen běžný provoz.

Implementační fáze projektu

Jednotlivé fáze projektu budou vycházet z doporučení ITIL, které pro zavádění ICT služeb (definuje následující procesy (fáze):

- Service Strategy
- Service Design
- Service Transition
- Service Operation
- Continual Service Improvement - CSI

Analytická – Service strategy

V rámci této fáze proběhne požadovaná **předimplementační analýza.** Součástí fáze je úvodní technický workshop technických specialistů uchazeče a zadavatele. Náplní workshopu je moderovaná diskuze zaměřená na technickou stránku projektu – zejména detailní specifikaci cílů projektu a očekávání jeho příjemců/uživatelů. Důležitou částí je specifikace objektivních podmínek, pravidel a zvyklostí, v nichž bude projekt realizován.

V analytické části specialisté uchazeče detailně zdokumentují stávající stav IT infrastruktury a aplikací včetně konfigurací, verzí a vzájemných vazeb.

Výstupem předimplementační analýzy pro bude dokument, který bude pokrývat minimálně následující oblasti:

a) Detailní popis stávajícího stavu, identifikaci slabých míst a bezpečnostních rizik, včetně vazeb na HW a SW systémy TC.

b) Způsob začlenění nabízených komodit do prostředí TC.

c) Síťová infrastruktura ve vztahu k plánovanému využití.

d) SAN infrastruktura ve vztahu k plánovanému využití.

e) Virtualizační infrastruktura (serverová, disková) ve vztahu k plánovanému využití.

f) Integrace nabízených softwarových systémů.

g) Rekonfigurace stávajících systémů.

h) Dopady implementace na dostupnost a funkčnost stávajících služeb.

i) Posouzení dopadů na non-IT technologie (spotřeba energií, tepelný výkon).

j) Požadované součinnosti zadavatele a jejich rozsah.

k) Návrh opatření k odstranění neshod zjištěných v průběhu analýzy.

- Návrhová – Service design

Na základě zdokumentovaného stavu jednotliví specialisté pod vedením architekta řešení navrhnou detailní postupy dosažení cílového stavu včetně potřebných konfigurací jednotlivých technologií a nezbytných součinností zadavatele. V průběhu návrhu postupů budou zvažována rizika spojená s uplatněním postupu. V případě nezanedbatelného rizika bude součástí postup návrh na odstranění či zmírnění rizika. Postupy budou zpracovány do dokumentu **Prováděcí dokumentace**, který bude zadavateli prezentován a předán ke schválení. Po schválení Prováděcí dokumentace bude uchazeč podle této dokumentace realizovat instalační fázi projektu. Dokument bude zahrnovat minimálně následující oblasti:

a) Detailní popis cílového stavu včetně funkcionalit jednotlivých částí systému,

b) Nutné a doporučené optimalizační a konfigurační změny dodávaných systému i všech navázaných systémů TC ORP (vSphere, LAN, SAN, zálohování, monitorování atd.),

c) Způsob zajištění potřebného HW a SW,

d) Způsob zajištění koordinace realizace předmětu plnění s běžným provozem,

e) Detailní návrh a popis postupu implementace předmětu plnění,

f) Detailní popis zajištění bezpečnosti informací,

g) Detailní harmonogram realizace včetně uvedení kritických milníků,

h) Návrh designu síťového a bezpečnostního řešení a jeho konfigurace,

i) Návrh designu aplikačních řešení,

j) Vazby na stávající systémy a jejich konfigurace,

k) Návrh akceptačních kritérií a akceptačních testů.

- Instalační - Service Transition

V rámci této fáze proběhne dodávka, montáž, oživení, konfigurace a otestování veškerých dodaných komponent (hw i sw) dle Prováděcí dokumentace. Pro zachování přehlednosti dokumentu neuvádíme popis této fáze jako soupis prováděných služeb dle Technické specifikace a potvrzení provedení každé z nich. Veškeré požadované služby budou uchazečem provedeny přesně dle poptávky. Pro prokázání jednoznačnosti navrženého implementačního postupu dále uvádíme chronologický seznam jednotlivých instalačních činností/kroků v doporučeném pořadí realizace, které povede k úspěšnému splnění předmětu plnění – je patrné, že projekt není vhodné (ani možné) implementovat v pořadí dle komodit a dokonce je nezbytné některé komodity implementovat ve více fázích proložených implementací jiné komodity. Všechny činnosti/kroky jsou řazeny sériově (za sebou), v průběhu implementace však budou některé z nich z důvodů urychlení implementace prováděny paralelně (souběžně), pokud to bude možné.

Implementační kroky budou vycházet z návrhové části a týkají se následujících oblastí (komodit):

- K1 - Rozšíření kapacit Technologického centra ORP

V rámci komodity provede uchazeče implementaci nových a rozšíření stávajících technologií TC ORP tak, aby byla zajištěna výkonná a spolehlivá systémová platforma pro implementaci a provoz řešení dalších komodit – především K2 a K3. Součástí rozšíření kapacit diskových polí bude i provedení odpovídajících změn konfigurace navázaných systémů – diskové a serverové virtualizace. V rámci rozšíření LAN infrastruktury uchazeč provede modernizaci „core" síťové vrstvy. Modernizací LAN tak bude navýšena kapacita páteřních tras na 10 Gb a doplněna možnost exportu síťových toků pro SIEM. Síťové toky bude exportovány přímo síťovými přepínači – jde o optimální řešení z pohledu využití investic a nízkých

nároků na správu. Pro začlenění nového serveru do TC ORP využije uchazeč stávající licence VMware vSphere a Veeam Backup & recovery poskytnuté zadavatelem. Implementací komodity nebude negativně ovlivněna dostupnost ani omezena funkčnost aplikací uživatelů.

V rámci komodity budou využita doporučení výrobců především v oblasti výkonové optimalizace serverové virtualizace Performance best practices vSphere, aby bylo zajištěno bezproblémové zpracování velkého množství logovaných informací v rámci komodity K2.

- K2 – SIEM & NBA

Z důvodů co nejjednodušší jednotné správy a minimalizace provozních nákladů zadavatele, bude nový SIEM s funkcí NBA **vybudován s maximálním využitím stávajících prostředků a technologií.** Řešení bude implementováno jako 2 virtuální appliance ve stávajícím prostředí VMware vSphere – jedna (hlavní) v lokalitě Moskevská, druhá v lokalitě U spořitelny. Logovaná data budou ukládána na virtualizované úložiště TC ORP a archivována na rozšířené síťové úložiště NAS. Pro sledování a logování síťových toků budou využity exportované síťové toky (netflow) ze síťových přepínačů implementovaných v rámci K1.

Při návrhu a implementaci nového systému SIEM s funkcí NBA budou uplatněna doporučení výrobce, tak jak jsou specifikovány v **best practices** https://www.alienvault.com/resource-center/webcasts/best-practices-for-configuring-ossim. Tím bude vedle kvalitní implementace také zajištěno, že nasazení SIEM & NBA nijak negativně neovlivní chod stávajících aplikací.

Systém SIEM & NBA bude navržen a konfigurován takovým způsobem, aby umožnil pověřeným pracovníkům přistupovat k systému a jím zpracovávaných údajům v režimu „pro čtení" a s možností tvorby vlastních pohledů či přehledů a jejich sad (tzv. dashboardů).

V rámci analytické, návrhové i implementační fáze budou realizovány následující kroky tak, aby byly beze zbytku naplněny cíle a očekávání Zadavatele vyplývající ze zadávací dokumentace:

a) Bude provedena detailní analýza – identifikace zdrojů dat, jejichž provozně bezpečnostní informace bude nutné popř. vhodné sbírat, korelovat a analyzovat

b) Budou vybrány zdroje dat z tzv. primárních a podpůrných (technických) aktiv zadavatele. K jejich určení bude využito Vyhlášky č.317/2014 Sb. o významných informačních systémech a jejich určujících kritérií přiměřeně uzpůsobených a aplikovaných na prostředí zadavatele (zadavatel neprovozuje významný informační systém). Dále bude pro určení zdrojů dat využito vstupního osobního setkání (workshopu) se správci provozovaných informačních a komunikačních systémů v rozsahu jednoho pracovního dne.

c) Budou navrženy a provedeny konfigurace dotčených a souvisejících systémů

d) Budou navrženy a provedeny akceptační testy, které zahrnou výkonové testy, testy archivace a obnovy logů a ověření detekce jejich neoprávněně modifikace.

Předimplementační analýza bude obsahovat následující oblasti specifické pro komoditu:

a) specifikace profilu pro každý napojovaný zdroj dat, včetně určení vhodné úrovně detailu logování, odpovídající jeho roli v infrastruktuře,
b) klasifikaci zdrojů informací pro stanovení priority události (stejná událost z různých zdrojů může mít různou prioritu) a z hlediska poskytovaných logů (obsažené informace, struktura logu),
c) doporučení nastavení logování pro jednotlivé zdroje,
d) výběr událostí a parametry jejich záznamů a metody sběru z jednotlivých zdrojů,
e) návrh parserů pro zdroje, které nebudou systémem přímo podporovány,

f) návrh doplňování logovaných informací z dalších zdrojů pro zlepšení jejich relevantnosti či srozumitelnosti,
g) metody a pravidla identifikace, zpracování a vyhodnocování událostí, návrhy korelací,
h) pravidla pro vznik varováni, upozornění, incidentů včetně priority,
i) doporučenou strukturu oprávnění a řízení přístupových práv
j) proaktivní a reaktivní procesy (aktivity, role, výstupy, doba odezvy) v případě výskytu varování, upozornění, incidentu a apod.
k) popis zajištění autentičnosti logů,
l) definice pohledů na události v konzoli uživatelů (např. setřídění událostí podle zdroje, typu, priority, stupně důležitosti, času vzniku apod.),
m) návrh zálohování konfigurace a dat,
n) návrh průběhu Zkušebního provozu pro ověření funkčnosti systému v reálném provozu,
o) návrh retence logů a archivů,
p) návrh způsobu napojení řešení na monitorovací systém uchazeče a definice procesů reakce, které jsou v souladu s platnou legislativou a bezpečnostní politikou MMKV,
q) popis monitorovaných aktivit přispívajících k naplnění požadavků dle zákona č.101/2000 Sb. v aktuálním znění a k naplnění požadavků dle Nařízení evropského parlamentu a rady EU 2016/679 o Zabezpečení zpracování osobních údajů (GDPR)

V průběhu instalační fáze budou provedeny následující implementační kroky:

- provedení výběru kritických bezpečnostních kontrol podle doporučení U.S. Centre of Internet Security (CIS) - SANS TOP20 CSC
- aplikování výběru na bezpečnostní framework ČSN ISO/IEC 27001:2014 a doplnění o další kontroly plně reflektující požadavky Vyhlášky 316/2014 sb., která je prováděcím pokynem Zákona č. 181/2014 sb. o kybernetické bezpečnosti
- nastavení definic zodpovědných osob a nastaveny konkrétní metriky
- nastavení sběr logů dle potřebných požadavků legislativ a shod tak, aby sledovaly jednotlivá rizika konkrétních aktiv - definici detekčních procesů
- definice procesů reakce, které jsou v souladu s platnou legislativou, ve shodě s regulatorními podmínkami a s bezpečnostní politikou a strategií zákazníka
- nastavení systému SIEM lokálně (v prostředí MMKV) včetně konfigurace potřebného hardware a dalších systémů pro provoz, sběr i ukládání logů
- integrace lokálního dohledového systému s centrálním dohledovým systémem (bezpečnostním dohledovým centrem) uchazeče
- zaškolení specialistů Zadavatele na užívání a základní obsluhu lokálního dohledového systému

Požadované služby provozní podpory řešení SIEM & NBA bude uchazeč provádět prostřednictvím vlastního specializovaného dohledového centra - tj. vyhrazených technických prostředků a specialistů určených a vyhrazených pro poskytování služeb bezpečnostního dohledu a řešení bezpečnostních incidentů. Dohledové centrum bude dále zajišťovat průběžné služby bezpečnostního monitoringu a dohledu:

- profylaxe systému každý měsíc
- provozní kalendář 9x5xNBD
- aktualizace a opravy systému
- průběžné aktualizace bezpečnostních a detekčních signatur
- zajištění bezpečného, úplného a nezpochybnitelného vyhodnocování a archivace logů ICT prostředí zadavatele a naplnění požadavků dle zákona č. 181/2014 Sb. (ZKB) a vyhlášky č.316/2014 Sb. (VKB), o kybernetické bezpečnosti, a to v platných zněních
- analýza logů a korelace událostí v reálném čase
- analýza událostí a identifikace možných incidentů v reálném čase

- alerting rizikových událostí či incidentů v reálném čase pomocí komunikačních nástrojů: mail, sms, telefon
- garantované zahájení řešení Kybernetického bezpečnostního incidentu (dále jen incident) technickým specialistou do 4 hodin od zjištění incidentu
- Service Desk pro řízení komunikace a průběhu služby - zakládání požadavků, proaktivní komunikace o jejich řešeních
- zajištění komunikace s třetímu stranami (NBU, NUKIB, CSIRT) při řešení bezpečnostních incidentů (v rámci řešení celého životního cyklu incidentu)
- průběžné změny a úpravy parametrů systémů a služeb pro zajištění trvalého zvyšování úrovně kybernetické bezpečnosti IT MMKV (přidání/úprava sledovaných hodnot a parametrů, přidání sledovaných aktiv atd.) a schopnosti detekce nových kybernetických hrozeb
- reporting - 1x měsíčně report o událostech a incidentech s návrhy systematických opatření, vzdálená prezentace do 1 hod – rekapitulace průběhu plnění, objasnění incidentů a rizik, doporučení opatření pro trvalé zvyšování úrovně kybernetické bezpečnosti IT MMKV.
- rozšířený reporting
    - měsíční "Asset discovery scan" - nová, detekovaná technická aktiva
    - měsíční "Vulnerability scan" - scan zranitelností technických aktiv
    - měsíční "Základní NBA scan" - základní přehled o stavu sítě a síťové komunikace, „top" komunikační žebříčky - kdo, s kým a jak (NBA - network behavior analysis)
- K3 – Správa identit

Systém pro správu identit IDM plně nahradí veškeré funkce stávajícího systému EOS (Evidence organizační struktury) a navíc zavede výrazně vyšší úroveň automatizace správy elektronických identit a integrace s klíčovými aplikačními systémy zadavatele. Při implementace komodity pro správu a řízení identit bude v rámci implementačního projektu zorganizována série workshopů na specifická témata řízení identit. Bude se jednat zejména o oblast představení možností a vlastností dodávaného systému IDM, představení možností napojení systému IDM na vybrané systémy zadavatele. Série workshopů bude zorganizována mezi týmem našich technických specialistů a vybraných klíčových specialistů na straně zadavatele. Cílem těchto workshopů bude získat od zadavatele veškeré potřebné informace pro vytvoření dokumentace analýzy zahrnující údaje potřebné k přípravě implementace IDM v prostředí zadavatele.

Analýza pro systém řízení identit bude zahrnovat následující části:

Analýza procesů a aplikací MMKV se zaměřením na oblast správy uživatelských účtů, přidělování oprávnění a rolí. V rámci této části naši specialisté zmapují stávající procesy a požadavky z oblasti správy identit na straně MMKV. Konkrétně se jedná o procesy nástupu nového zaměstnance a přiřazení oprávnění v systémech, se kterými potřebuje zaměstnanec pracovat. Dále pak proces odchodu zaměstnance a deaktivace jeho přístupových účtů, změny organizačního začlenění zaměstnance, správa oprávnění pro externí subjekty, proces přiřazování a změny hesla, proces přiřazování a změny uživatelského jména, atd.

Analýza požadavků MMKV zasílaných centrálním informačním systémům, základním registrům a dalších informačních systémů s požadavkem na autorizaci a autentizaci. V rámci této části naši specialisté zmapují stávající procesy a požadavky z oblasti správy identit na straně MMKV ve vztahu k centrálním systémům jako ISZR, RPP, JIP, atd. Konkrétně se jedná o procesy, v rámci kterých je spravována evidence agend a činnostních rolí pro komunikaci orgánu veřejné moci se základními registry. Dále budou zmapovány systémy, které na MMKV komunikují se základními registry.

Technologický popis stávajících technologií s vazbou na systém správy identit. V rámci této části naši specialisté zmapují stávající technologie a systémy s vazbou na systém správy identit. Jedná se zpravidla o technologie provozu IT infrastruktury zadavatele a jednotlivé systémy významné z hlediska správy identit jako personální systém, adresářová služba, emailový server, spisová služba a další. Naši specialisté rovněž provedou společně se zástupci specialistů ze strany zadavatele rozbor dat vázaných na správu identit v jednotlivých systémech zadavatele.

Analýza možností správy výstupních struktur. V rámci této části naši specialisté přestaví možnosti výstupních struktur systému. Jedná se zejména o reporty aplikačních rolí, historizační reporty identit, report pro ohlášení působnosti k nové agendě nebo agendové činností roli, simulační reporty platformy IDM atd.

Analýzu evidenčních údajů a logů. V rámci této části naši specialisté přestaví možnosti správy evidenční údajů v systému IDM a možnosti vytváření logů v systému IDM. Dále bude představena práce s logy systému IDM.

Návrh životního cyklu identity uživatelů. V rámci této části naši specialisté dle sesbíraných vstupů navrhnou proces životního cyklu identit platný pro zavedení systému IDM.

Model organizační struktury. V rámci této části naši specialisté zmapují stávající organizační strukturu na straně MMKV. Bude proveden rozbor jednotlivých částí organizační struktury a jejich částí – odbory, oddělení včetně toho, ve kterých systémech je organizační struktura spravována a jakými způsoby.

Seznam systemizovaných pracovních pozic a přiřazení pracovníků k pracovním pozicím. V rámci této části naši specialisté zmapují stávající hierarchii systematizovaných stávajících pozic na straně MMKV. Bude proveden rozbor jednotlivých vazeb nadřízenosti a podřízenosti pracovních pozic, obsazenost pracovních pozic, mechanizmy změn nastavení pracovních pozic. Bude přestaven návrh navazovat uživatelská oprávnění na pracovní pozice.

Atributy poskytované personálním systémem v souladu s potřebami obsluhovaných systémů a návrh jejich využití. V rámci této části naši specialisté zmapují údaje spravované v personálním systém (evidence organizační struktury, pracovních pozic, osob). Bude proveden rozbor, zda jsou tato data dostatečná pro řízení oprávnění systémem IDM napříč systémy MMKV a centrálními systémy.

Manažerský souhrn vhodný pro prezentaci výstupů analýzy vedení MMKV. V rámci předimplementační analýzy bude vypracován manažerský souhrn obsahující hlavní body vyplývající z analýzy stávajícího stavu včetně návrhu metodických, procesních a technických opatření pro implementaci systému IDM.

Výstupy z jednotlivých částí budou zpracovány do dokumentu **Přeimplementační analýza**, který bude zadavateli prezentován a předán ke schválení. Po schválení této dokumentace bude uchazeč podle této dokumentace realizovat návrhovou fázi projektu. V rámci návrhové fáze uchazeč vypracuje prováděcí dokumentaci popisující návrh cílového stavu implementace systému IDM. Dokumentace bude vycházet z dokumentace předimplementační analýzy a bude zahrnovat následující části:

Návrh implementace systému IDM. V rámci této části naši specialisté popíší návrh implementace systém IDM pro MMKV. V návrhu řešení implementace IDM bude zohledněn navržený cyklus správy identit z dokumentace přeimplementační analýzy a další vstupy z předimplementační analýzy. Návrh implementace systému IDM bude obsahovat návrh a konfiguraci implementovaného systém IDM, návrh implementace algoritmu pro správu uživatelský jmen, hesel a dalších potřebných nastavení systému IDM.

Návrh napojení na požadované systémy ze strany MMKV. V rámci této části naši specialisté popíší návrh implementace napojení systému IDM na požadované systémy ze strany MMKV. U každého popisovaného napojení bude uveden směr synchronizace dat mezi systém IDM a požadovanými systémy, rozsah synchronizovaných dat, režimy synchronizace a tabulka mapování a transformace údajů, atributů přenášených v rámci jednotlivých synchronizací.

Návrh a provedení akceptačních testů. V rámci této části naši specialisté popíší detailní návrh akceptačních kritérií, které budou obsahovat návrh výkonových, integračních a testů případů užití systému IDM.

Návrh požadovaných úprav stávajících systémů. Při implementaci systému IDM a jeho napojení na systémy v organizaci je zpravidla nutné zajistit úpravu dat a provedení instalace potřebných komponent na straně třetích systémů. V rámci této fáze budou vydefinovány požadavky na úprav těchto dat případně systémů pro dosažené metodicky vhodného a konzistentního stavu dat požadovaného pro řízení identit.

V rámci instalační fáze komodity pro správu a řízení identit budou provedeny následující aktivity:

Příprava implementačního balíku IDM. V rámci této aktivity naši specialisté připraví implementační balík pro provedení instalace systému IDM v prostředí MMKV. Tento instalační balík vznikne na základě podkladů a dokumentace předimplementační analýzy a prováděcí (návrhové) dokumentace. Instalační balíček bude následně otestován našimi specialisty v našem interním vývojovém a testovacím prostředí.

Provedení nezbytných součinností na straně napojovaných systémů ze strany IDM. Při implementaci systému IDM a jeho napojení na systémy v organizaci je zpravidla nutné zajistit úpravu dat a provedení instalace potřebných komponent na straně třetích systémů. V rámci této fáze budou vydefinovány požadavky na úpravu dat těchto systémů pro dosažení metodicky vhodného a konzistentního stavu požadovaného pro řízení identit.

Instalace IDM do prostředí MMKV. V rámci této aktivity naši specialisté nainstalují připravený instalační balík do prostředí MMKV. Dále bude zajištěno ve spolupráci se zadavatelem a dodavateli systémů třetích stran provedení požadovaných úprav dat v systémech MMKV pro efektivní řízení identit.

Provedení testů systému IDM. V rámci této aktivity naši specialisté provedou testy systému IDM v prostředí MMKV. Následně budou ve spolupráci s MMKV provedeny akceptační testy řešení IDM.

Provedení simulačních synchronizací. V rámci této aktivity naši specialisté provedou simulační synchronizace systému IDM v prostředí MMKV na požadované napojované systémy. Výstupem této aktivity budou vytvořeny rozdílové reporty poukazující na případné nekonzistence identitních dat v jednotlivých napojovaných systémech. Následně budou ve spolupráci s MMKV provedeny aktivity pro odstranění případných datových nekonzistencí.

Spuštění řádných pravidelných synchronizací. Po uvedení identitních dat do souladu v rámci předchozí aktivity, bude možné za naší asistence nastavit úlohy pravidelných automatických synchronizací IDM s požadovanými systémy.

- Doporučené postupy

Pro kvalitní návrh a implementaci systému IDM budou využity osvědčené a doporučené postupy (tzn. best practice – nejlepší praktiky).

Správa uživatelských rolí. V rámci řízení oprávnění IDM umožňuje centrální správu uživatelských rolí, tj. zařazení uživatele do odpovídající role v daném systému nebo aplikaci. Aplikační role je možné v IDM přiřazovat na koncové uživatele. IDM navíc umožňuje přiřazovat aplikační role na systematizovaná místa, organizační jednotky a skupiny. Aplikační role přiřazené na tyto referenční údaje následně „propadávají" na koncové uživatele, kteří jsou na daných organizačních jednotkách, systematizovaných místech a skupinách včleněni. Mechanismus implementovaných konektorů pak zajišťuje, že jsou identity a jejich změny včetně odpovídajících rolí a oprávnění vypropagovávány z IDM do relevantních systémů a to v odpovídajícím formátů a rozsahu definovaném pro každý jednotlivý systém samostatně.

Import aplikací a aplikačních rolí. IDM umožňuje správu číselníku aplikací a dále pak správu číselníku aplikačních rolí pro dané aplikace. V IDM je možné aplikační role evidovat a spravovat ručně přes portál. Dále je možné do IDM synchronizovat seznam aplikačních rolí přes rozhraní webových služeb IDM. Služba importu aktualizuje aplikace a aplikační role požadované skupiny aplikací. V případě, že není zadána na vstupu skupina aplikací, tak je aktualizována pouze samostatná aplikace. V případě, že je na vstupu předaná skupina aplikací, která neexistuje, vytvoří se nová skupina aplikací. Je-li v seznamu aplikací nová aplikace dosud nezaevidovaná v IDM, vytvoří se v IDM nový záznam. Chybějící aplikace se automaticky nedeaktivují. Pro aplikační role příslušné aplikace platí, že nové role na vstupu se vytvoří v IDM, chybějící se deaktivují.

Správa skupin a členství v skupinách adresářové služby. IDM umožňuje správu skupin a správu členství v skupinách adresářové služby. IDM umožňuje evidenci skupin, které mohou, ale nemusí být synchronizovány s adresářovými služ-

bami jako například Active Directory, LDAP, atd. V IDM je možné následně začleňovat jednotlivé identity do těchto skupin buď ručně v portálu IDM nebo automaticky podle definovaných pravidel. IDM umožňuje následně synchronizovat skupiny a členství ve skupinách do cílové adresářové služby. IDM dále umožňuje iniciační načtení seznamu skupin a uživatelských účtu z adresářové služby pro naplnění evidence v IDM.

Automatické zařazení uživatelů do skupin a aplikační rolí. Kromě ručního zařazení uživatele do skupiny administrátorem IDM může být uživatel při zápisu změn zařazen do skupin uplatněním pravidel pro automatické zařazení do skupin a aplikačních rolí. Pro automatické zařazení nastaví administrátor v administrátorské konzoli pravidel - sadu pravidel, podle kterých se na základě atributů uživatele vyhodnotí sada uživatelských skupin, aplikačních rolí, do kterých má být uživatel zařazen. Automatické zařazení uživatele do skupiny může být nastaveno podle různých atributů uživatele – např. zařazení do organizační jednotky, na pracovní místo a dalších atributů resp. kombinace atributů uživatele. Spouštění pravidel je definováno jako synchronizovaný systém, do něhož lze nastavit interval spuštění změnové nebo kompletní synchronizace (vyhodnocení pravidel). Na základě vyhodnocení sady pravidel se uživatelé zařadí do příslušných skupin, aplikačních rolí. Ruční zařazení do skupiny (administrátorem) má přednost před automatickým zařazením a není automatickým procesem dotčeno. Uživatelsky (administrátorem) je možné přepnout příznak automatického / ručního zařazení.

Výsledné stavy vyhodnocení pravidel:

- Beze změny
- Nové skupiny, role – uživatel se zařadí
- Chybějící skupiny, role – uživatel se vyjme. Nelze automaticky vyjmout ze skupiny nebo role, která má „automaticky = false".

Změna zařazení do skupiny se promítne s okamžitou platností – po aplikaci pravidel.

Stupně komunikace IDM s připojenými systémy. Řešení IDM umožní spravovat životní cyklus všech identit v rámci infrastruktury zadavatele. Napojení jednotlivých IS a aplikací IDM může být implementováno v následujícím rozsahu:

- Plná integrace (správa identit) – kompletní správa identit včetně nastavení konkrétních práv a rolí probíhá pouze v systému IDM a IS či aplikace přebírá toto nastavení, např. procesy založ, edituj, smaž uživatele, aktivuj/deaktivuj přístup, přiřaď/odeber konkrétní roli a práva.
- Částečná (poloautomatická) správa – v IDM se nastavují přístupové údaje uživatele (založ, edituj, smaž, zablokuj), v integrovaném IS či aplikaci se definují konkrétní role a práva.
- Nepřipojené (virtuální) aplikace – za využití IDM je požádáno o založení/změnu/smazání přístupu, rolí a práv, nastavení je však nutné provést „ručně" administrátorem – aplikace není přímo integrována. IDM obsahuje notifikační konektor, který bude simulovat napojení aplikace, která zatím není napojena na IDM. Pokud administrátor nebo automatické pravidlo přidají nebo odeberou identitě roli v IDM z této aplikace nebo změní identitu, pošle se emailová notifikace definovanému příjemci (administrátorovi) aplikace. Příjemce následně může na základě této notifikace provést požadované nastavené v dané aplikaci.

IDM rovněž implementuje plnou integraci s adresářovou službou včetně správy skupin, organizačních jednotek a příslušnosti uživatelů do těchto objektů. V případě, že jednotlivé aplikace využívají pro řízení autentizace a autorizace adresářové služby, tak je možné přes IDM tímto způsobem řídit plnou nebo částečnou správu identit i v těchto aplikacích.

- K4 – Školení kybernetické bezpečnosti

Komodita školení vzhledem ke svému charakteru (soubor školení a testů) bude realizována odlišným způsobem od ostatních komodit (nebude probíhat implementace) – dle vzdělávací metodiky. Vzdělávací metodika je proto popsána v samostatném dokumentu.

Součinnosti

Časová náročnost

Nezbytnou podmínkou úspěšné implementace je kvalitní součinnost specialistů, ale i uživatelů zadavatele. Uchazeč si je vědom velkého časového vytížení zaměstnanců zadavatele, proto omezí požadavky na součinnost na nezbytné minimum. Vzhledem k rozsahu projektu předpokládáme následující časové nároky na činnosti, u nichž je nezbytné součinnost (účast) specialistů zadavatele:

- Projektové schůzky, úvodní workshopy – 16 hod
- Připomínkování, schvalování dokumentace – 8 hod
- Asistence při nastavení sběru logů specifických aplikací zadavatele – 12 hod
- Akceptační testy – 8 hod
- Školení – 24 hodin
- Jiná součinnost (zajištění přístupů, poskytnutí dokumentací apod.) – 10 hod

Vedle technických certifikací budou všichni specialisté zájemce i jeho subdodavatelé disponovat praktickými zkušenostmi z implementací technicky i rozsahem obdobných projektů, které uplatní v analytické, návrhové, instalační i provozní fázi projektu.

Dodávaný systém IDM je prověřený a zavedený systém v oblasti státní samosprávy a disponuje již připravenými moduly a konektory požadovanými ze strany zadavatele, například konektor na personální systém FLUX, systémy Ginis, Active Directory, Exchange, JIP, RPP atd. Díky tomu odpadne režie spojená s nutným vývojem těchto modulů a konektorů, která by do jisté míry nevhodně navýšila požadavky na kapacitu specialistů na straně zadavatele. Vlastnosti hotového a připraveného řešení jsme schopni demonstrovat v rámci případného požadovaného předvedení funkčního vzorku (prototypu).

Odborná náročnost

V rámci požadované součinnosti nebudou po zaměstnancích – zejména administrátorech – zadavatele požadovány žádné speciální odborné znalosti či dovednosti nad rámec aktuálně rutinně prováděných činností. Klíčovým přínosem administrátorů pro úspěch projektu je celková znalost prostředí zadavatele, způsobů využívání IT technologií, pracovních zvyklostí uživatelů a technických omezení či slabých míst stávajících technologií a řešení.

Podklady pro hodnocení

Doplňující informace implementačního postupu, členěné dle bodů pro hodnocení kvality implementačního postupu.

Popis implementačního procesu

Metodika implementace zohledňuje potřeby zadavatele v plném rozsahu, obsahuje detailní a jednoznačný popis postupu uchazeče při realizaci předmětu plnění, zcela pokrývající požadavky ZD.

50 bodů

Uchazeč předkládá detailně propracovaný, zcela vyhovující a jednoznačný postup realizace předmětu plnění. Navržený postup v míře a detailu danými vstupními informacemi popisuje jednoznačný postup realizace předmětu plnění v členění

po jednotlivých krocích, ze kterých je patrné naplnění zadání. Uchazeč v nabídce předkládá podrobný popis implementačního procesu tak, aby splnil technická kritéria a obecně platné technické předpisy a normy. V rámci popisů procesů a služeb uchazeč specifikuje i procesy nad rámec běžného uživatelského komfortu. Splněním technických kritérií uchazeč rozumí zprovoznění a nastavení dodaných technologií jednak v souladu s naplněním požadavků zadavatele na provedení služby či konkrétní funkčnost a jednak v souladu s doporučenými postupy výrobců, které de facto reprezentují technické předpisy pro používání dodaných technologií. Dodržování obecných technický norem a předpisů (typicky Vyhláška č. 50/1978 Sb a další) je dáno certifikacemi o zavedení systém řízení jakosti uchazeče a jeho subdodavatelů dle ISO 9001 a dalších – http://www.autocont.cz/o-spolecnosti/rizeni-kvality

- Kompatibilita se současným prostředím

Metodika implementace zohledňuje stávající prostředí zadavatele v plném rozsahu, z metodiky jednoznačně vyplývá, že implementované řešení je plně kompatibilní se současným prostředím zadavatele.

20 bodů

Uchazeč v nabídce prokazuje, že implementované řešení je plně kompatibilní se současným prostředím zadavatele. Technická kompatibilita navrženého řešení je splněna ve všech bodech podstatných pro bezproblémovou funkčnost celé inovované ICT infrastruktury:

- Nabízené servery jsou od stejného výrobce jako stávající, jsou plně kompatibilní se zadavatelem provozovaným Blade šasi do kterého budou vloženy – je zaručena plná kompatibilita se stávajícími servery a jejich správou
- Nabízené síťové prvky jsou od stejného výrobce jako stávající - je zaručena kompatibilita na úrovni technické a funkční (VLAN, porty atd.) i na úrovni managementu pro snadné osvojení správy administrátory zadavatele
- Nabízené rozšiřující komponenty do stávajících systémů jsou originální výrobky výrobce serverů – je zaručena technické kompatibilita
- Nabízené rozšiřující disky do stávajících úložišť HP MSA jsou originální výrobky výrobce – je zaručena plná technická kompatibilita
- využívána serverová virtualizační technologie VMware vSphere. Systém IDM je možné provozovat na této technologii.
- systém IDM bude využívat pro vlastní perzistenci dat stávající databázový server Microsoft SQL Server.
- systém IDM obsahuje pokročilý konektor na stávající emailový server Exchange.
- systém IDM obsahuje pokročilý konektor na stávající Active Directory.
- systém IDM obsahuje pokročilý konektor na Active Directory, přes který je možné řídit oprávnění v stávajícím systému MS Sharepoint.
- systém IDM obsahuje pokročilý konektor na systém FLUXPAM.
- pro správu dokumentů a spisů je využívána elektronická spisová služba AthenA s rozšiřujícím modulem iUsnesení pro správu dokumentů rady a zastupitelstva (PilsCom s.r.o.). IDM obsahuje konektory na běžné a rozšířené spisové služby.

- Optimalizace zachování a využití stávajících investic

Metodika implementace zohledňuje potřeby zadavatele v plném rozsahu, obsahuje detailní a jednoznačný popis postupu uchazeče při optimalizaci zachování a využití stávajících investic, zcela pokrývající požadavky ZD.

10 bodů

Uchazeč v nabídce prokazuje, že popsaný postup implementace řešení optimalizuje zachování a využití stávajících investic. S výjimkou prvků vhodných k náhradě (EOS) nebude vyřazen žádný stávající ICT prvek. Naopak implementací

nových technologií (SIEM, IDM) dojde k lepšímu využití stávajících zařízení a systémů. Významným způsobem vzroste úroveň automatizace správy ICT prostředí a úroveň jeho zabezpečení proti kybernetickým hrozbám.

Navržený postup implementace spolu s nabízenými produkty velmi úzce navazuje na současný stav (využívá maximum dostupných prostředků a technologií) a výrazným způsobem rozšiřuje a vylepšuje vlastnosti současné ICT infrastruktury tak, aby byla eliminována slabá místa současného stavu a současně byly doplněny funkce a vlastnosti odpovídají současným trendům a požadavkům v ICT

- Uplatnění doporučených postupů

Metodika implementace zohledňuje potřeby zadavatele v plném rozsahu, obsahuje detailní a jednoznačný popis uplatnění doporučených postupů výrobců dodávaných zařízení a tzv. best practice (nejlepších praktik) při implementaci těchto typů zařízení do prostředí zadavatele.

10 bodů

Uchazeč v nabídce prokazuje znalost a uplatnění doporučených postupů výrobců a tzv. best practice (nejlepších praktik). Navržené implementační kroky prokazují znalosti doporučených postupů např. instalační postup IDM a SIEM. Kompletní soupis použitých doporučených postupů je dle mínění uchazeče nad rámec určení tohoto dokumentu (jde o desítky), výše v textu jsou uvedeny ty nejdůležitější odkazy. Uplatnění nejlepších praktik je patrné z navržených implementačních kroků

- Minimalizace kapacitní náročnosti

Metodika implementace zohledňuje potřeby zadavatele v plném rozsahu, postup implementace minimalizuje kapacitní náročnost na zadavatele (zajištění součinnosti, tj. zajištění personálních kapacit zadavatele) při realizaci předmětu plnění.

10 bodů

Uchazeč minimalizuje kapacitní náročnost na zadavatele v oblasti administrativní a organizační (viz. Řízení implementace) i v oblasti časové a odborné náročnosti (viz. Součinnosti)

- Shrnutí

Celkově z popisu implementačního postupu vyplývá, že nabízený postup implementace povede k úspěšnému splnění předmětu plnění a naplnění veškerých požadavků zadavatele.

- Obsah kurzu

Tematické obsahy jednotlivých vzdělávacích aktivit **zohledňují všechny požadavky** na tematický obsah vzdělávání (kurzů). Viz Příloha č.2
100 bodů

- Metodika vzdělávání
  - Interaktivní přístup výuky

Metodika vzdělávání zohledňuje potřeby cílové skupiny a využívá vhodné didaktické postupy – vzdělávací kurzy obsahují interaktivní styl výuky, která aktivně zapojuje účastníky vzdělávacího kurzu do procesu vzdělávání tak, že je metodikou jasně a zřetelně zaručen. Viz Příloha č.2
33 bodů

○ Praktická forma výuky

Metodika vzdělávání zohledňuje potřeby cílové skupiny a využívá vhodné didaktické postupy – vzdělávací kurzy obsahují propojení výuky s praktickými zkušenostmi účastníků vzdělávacího kurzu. Viz Příloha č.2
34 bodů

○ Způsob ověření získaných dovedností

Metodika vzdělávání zohledňuje potřeby cílové skupiny a využívá vhodné didaktické postupy – vzdělávací kurzy obsahují metody pro efektivní ověření získaných dovedností účastníka vzdělávacího kurzu. v
33 bodů

• Studijní materiály

Studijní materiály zohledňují potřeby cílové skupiny a využívají vhodné didaktické postupy – studijní materiály **obsahují vzdělávací obsah, který vychází z tematického obsahu vzdělávacích aktivit.** Viz Příloha č.2
100 bodů

• Další hodnocené parametry

Hodnocené parametry			
Parametr	**Popis**	**Uchazeč popíše způsob naplnění tohoto hodnoceného parametru včetně značkové specifikace nabízených dodávek**	**Uchazeč uvede odkaz na přiloženou část nabídky, kde je možné ověřit naplnění parametru**
Snížení nároků na správu systému			
1	Systém pro správu identit komodity K3 bude využívat pro ukládání dat databázový server MS SQL	Systém pro správu identit komodity K3 bude využívat pro ukládání dat databázový server MS SQL	Kapitola 6.1 Technické řešení
Uživatelské přívětivost a snížení nároků na správu			
2	Kompletní uživatelské prostředí i prostředí pro běžnou správu a konfiguraci systému pro správu identit komodity K3 bude v českém jazyce	Kompletní uživatelské prostředí i prostředí pro běžnou správu a konfiguraci systému pro správu identit komodity K3 bude v českém jazyce	Kapitola 6.1 Technické řešení

8.2 Příloha č.2 Specifikace školení a metodika vzdělávání

Proškolení všech zaměstnanců úřadu na problematiku kybernetické bezpečnosti. V současné době má zadavatel 179 zaměstnanců. Před zahájením školení proběhne test phishingu (podvodné a nebezpečné jednání, typicky škodlivá příloha v emailu), na školení bude provedeno seznámení s výsledky a vysvětlení, jak se bránit phishingu, po cca 5-6 měsících bude provedeno opakované provedení testu a vyhodnocení.

Kurz je určen pro všechny zaměstnance městského úřadu. Obsah školení bude:

1. Legislativní rámec.
2. Bezpečnostní politika – informace – ZOOU (zákon o ochraně osobnách údajů).
3. Bezpečnostní směrnice – proškolení na bezpečnostní směrnici organizace.
4. Škodlivý software – jak se projevuje, jaké jsou druhy a jak se bránit, preventivní chování, praktické cvičení antivirový program – provádění kontroly.
5. Elektronická komunikace s úřady: datová schránka – co to je, k čemu slouží, zřízení a práce s datovou schránkou, elektronický podpis – co to je, jak s ním pracovat, jeho výhody a nevýhody.
6. Data vs. informace, práce s daty, šifrování, praktický úkol šifrování dat.
7. Zálohování, archivace a mazání dat, praktický úkol zálohování dat.
8. Sociální sítě a chat – chatování, Skype, Facebook, výhody a rizika, praktické ukázky.
9. Přístup k síti – PIN / heslo a jeho uložení, správné heslo.
10. Ztráta identity se mě (ne)týká?
11. Mailování bezpečně – co e-mailem nikdy neposílat, spamy, phishing, hoax, bezpečné přihlášení/odhlášení, zálohování e-mailů, phishing.
12. Kyberšikana – co to je, jaké jsou její formy a jaká preventivní opatření.
13. Závěr /obecný bezpečnostní test.

Před zahájením školení bude obsah kurzu upraven dle specifické bezpečnostní politiky organizace, uchazeč provede kompletní revizi a aktualizaci stávající bezpečnostní směrnice zadavatele a bude nastaveno prostředí webináře. Vzdělávací kurz bude obsahovat také seznámení s nařízením GDPR (Obecné nařízení o ochraně osobních údajů (angl. General Data Protection Regulation) v rozsahu potřebném pro základní seznámení s problematikou GDPR (viz např. https://www.uoou.cz/gdpr-a-role-uoou/d-23082). Zadavatel má právo schválit konkrétní obsah vzdělávacího kurzu před zahájením realizace předmětu plnění.

Kurz je koncipovaný jako kombinace e-learningového vzdělávací program (webináře) a prezenčních workshopů.

Uchazeč zajistí studijní materiál pro prezenční workshopy. Obsah studijního materiálu bude odpovídat rozsahu vzdělávaného tématu. Studijní materiály budou obsahovat mimo jiné kontakt na odborné realizátory (lektory) vzdělávání tak, aby je v případě potřeby mohli účastníci kontaktovat i po skončení kurzu. Studijní materiály budou obsahovat všechny povinné znaky publicity dle Operačního programu zaměstnanost. Studijní materiály budou poskytnuty všem účastníkům vzdělávací aktivity v elektronické podobě. Současně budou studijní materiály poskytnuty v listinné podobě účastníkům, a to přímo na daném workshopu.

E-learningový webinář, jehož obsahem budou prezentované informace a bude zakončen povinným obecným bezpečnostním testem v rozsahu 20 otázek s možností volby mezi připravenými odpověďmi, bude dostupný na internetu po

dobu 3 měsíců od prvního workshopu (očekává se průběžné skládání testů skupinami zaměstnanců, kteří budou absolvovat konkrétní běh školení). Každý zaměstnanec absolvuje školení formou webináře včetně závěrečného testu. Po 5-6 měsících budou muset zaměstnanci provést opakovaný test a případně pro připomenutí zopakovat webinář (bude přístupný po dobu 3 měsíců od opakovaného testu). Předpokládá se, že každý účastník bude absolvovat e-learningový webinář samostatně.

Funkcionality systému pro realizaci e-learningových webinářů:

- Hromadný e-mailing pro rozesílání pozvánek do kurzů, upozornění na expirace certifikátů, avíza o zahájení a ukončení kurzu nebo jiné zprávy.
- Přizpůsobitelné a intuitivní uživatelské rozhraní.
- Pokročilý testovací engine s možností řídit pohyb uživatele ve webináři.
- Možnost ochrany proti podvádění u testů zamícháním otázek a odpovědí, možnost nastavit náhodné generování vybraných otázek.
- Možnost automatického i ručního vyhodnocení testů.
- Možnost jednorázového importu uživatelů do systému nebo možnost, aby se uživatelé mohli registrovat sami.
- Možnost vystavení certifikátů o absolvování.
- Podrobné reporty.
- Využití technologie Google Analytics pro sledování návštěvnosti a chování uživatelů.
- Podpora pro mobilní zařízení.

Test phishingu bude realizován pro každého zaměstnance dvakrát – jednou před kurzem a podruhé po 3 měsících po ukončení kurzu, bude tak prakticky ověřeno posílené bezpečnosti a případné problémové oblasti budou následně probrány na prezenčním workshopu.

Prezenční workshop bude v délce 4 výukových hodin, realizace bude po skupinách max. 50 osob. Každý účastník tedy absolvuje e-learning v rozsahu 2 výukových hodin a dále prezenční workshop v rozsahu 4 výukových hodin, účastník tedy absolvuje celkem 6 výukových hodin. Workshopy budou probíhat v sídle zadavatele.

Obecné parametry

Pro každý workshop (každé prezenční školení) poskytovatel zpracuje prezenční listinu, která bude vlastnoručně podepsána účastníky kurzu a lektorem/lektory. Všichni účastníci po absolvování vzdělávacího programu obdrží osvědčení o účasti. Poskytovatel zajistí rovněž fotodokumentaci aktivity, která bude prokazatelně evidovat, že aktivita proběhla – min. budou zaznamenáni lektoři, účastníci workshopu, aktivity.

Prezenční listiny z proběhlých aktivit budou zahrnovat:

- datum realizace aktivity
- jméno a příjmení osob účastníků kurzů
- název poskytované aktivity
- místo poskytování aktivity
- podpis účastníků

Veškeré dokumenty, které budou vytvořeny v rámci plnění, budou splňovat povinné prvky publicity Operačního programu zaměstnanost.

Součástí předmětu plnění je provedení evaluace. Cílem je získání zpětné vazby ze strany cílové skupiny, která je zapojena do projektu a zúčastní se vzdělávacích aktivit. Průběh evaluace bude probíhat dle uvážení poskytovatele, a to např. formou dotazníku ihned po ukončení dílčí části. Výstupy budou Zadavateli dodány v elektronické podobě ve formátu MS Word/ Excel nejpozději do 7 dnů od ukončení každé dílčí části.

Zadavatel má možnost po dohodě s Dodavatelem přizpůsobit skupiny účastnící se vzdělávání, tj. počet i složení účastníků, stanovit termíny jednotlivých aktivit.

Zadavatel má možnost před podpisem smlouvy ověřit funkčnost nabízených e-learningových webinářů a shodu nabízené funkcionality se ZD.

Každý den se na vaše uživatele valí lavina podvodných emailů. Jednou předstírají, že jsou z České pošty, jindy zase, že obsahují faktury. Stačí jedno kliknutí a počítač i potažmo celá vaše síť je nakažena. Je jedno, jestli bude počítač uzamčen vyděračským Cryptolockerem nebo se změní v zombie, která bude čekat na povel neznámého zločince, vždy utrpíte škodu. Škodu na majetku, času, reputaci. Škodu, která znamená ztrátu produktivity a peněz!

Bezpečnost je omezena nejslabším článkem a tím je vždy člověk. Jedno kliknutí jediného uživatele může znamenat definitivní ztrátu dat a informací, projektů, obchodu, času, peněz... Můžete své uživatele připravovat a školit jak se mají chovat a jak čelit podvodným emailům, nicméně nejde to „jedním uchem dovnitř a druhým ven"? Přesvědčte se, jestli bezpečnostní školení a upozornění jsou skutečně účinná a jestli jsou provedená bezpečnostní opatření dostatečně efektivní. Můžete vynakládat spoustu prostředků (čas, peníze,...), ale pokud nebudou mít efekt, jsou to vlastně ztracené peníze a při úspěšném útoku bude ztráta ještě větší. Budujte tedy bezpečnostní povědomí svých uživatelů a přijímejte opatření tak, aby byla účinná.

Uživatelé Zadavatele jsou testováni na odolnost vůči phishingu (cílenému útoku prostřednictvím emailu). Je připraven jeden nebo více emailů, které předstírají, že jsou legálními emaily a ty jsou rozeslány na vybrané uživatele Zadavatele. Emaily obsahují v těle odkaz (tak jak je tomu u skutečných phishing emailů) a pokud uživatel na odkaz klikne je zaregistrován pro další vyhodnocení. Emaily pro hodnověrnost mohou falšovat libovolného odesilatele včetně vizuálního stylu.

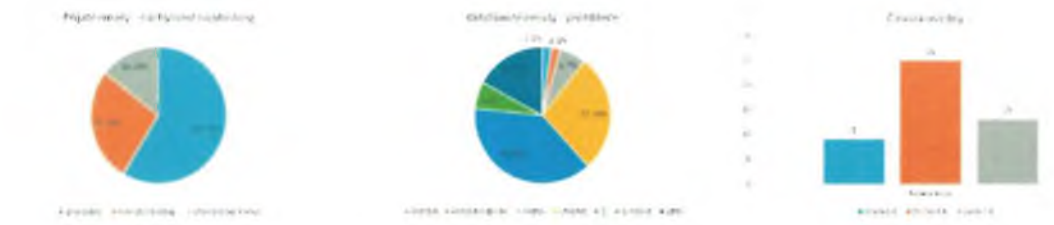
Zadavatel získá představu nakolik jsou jeho uživatelé zranitelní phishing útokem.

Klíčové charakteristiky

- Je zaznamenáno otevření a kliknutí na email.
- Je zaznamenáno jméno uživatele, prohlížeč, kterým otevíral odkaz a IP adresa.
- Je možné test rozprostřít do potřebného časového okna, test je možné opakovat a tím sledovat efekt školení uživatelů.
- Možnost vytvořit libovolný email a info pro uživatele, který na link kliknul.

Zpracování výstupu

Výsledky jsou vyhodnoceny a je zpracována zpráva.



Příklady výstupů

8.2.1 Příklad phishingového mailu

Odesilatel: [redacted]

Předmět: Rozjíždíme Vánoce!!!

ROZJÍŽDÍME VÁNOCE!!!

Všechny dárky vyřešíte na Alza.cz

Možná, že je ještě brzy na Vánoční nákupy, ale zaregistrujte se pro svoji Vánoční slevu už teď. Za registraci získáte slevu 20%. Takové Vánoce ještě nikdy nebyly.

Neváhejte – registrace je možná jen do 28.10. a pak už to rozjedeme ve velkém.

Registrace je možná zde: www.alze.cz/akce/rozjizdime_vanoce_reg

Další informace naleznete zde: www.alze.cz/akce/rozjizdime_vanoce

Slevy na Vás nepočkají!!!

Více zde >>

Splátky bez navýšení

Na velké domácí spotřebiče

© 1994 - 2016 Alza.cz a.s. info@alza.cz

8.2.2 Ukázka studijních materiálů – zákon o ochraně osobních údajů

Musíme osobní údaje nějak zvlášť chránit?

1950: Evropská úmluva o ochraně lidských práv a základních svobod

1981: Úmluva o ochraně osob se zřetelem na automatizované zpracování osobních dat

1993: Ústava (ČR)

1995: směrnice EU (mezinárodní úprava)

2000: zákon o ochraně OÚ (národní úprava ČR)

2016: **nařízení EU** (mezinárodní úprava)

- Mezinárodní významný den:

28. leden (2017) - Den ochrany osobních údajů

AUTOCONT

Jaké „osobní údaje“ zpracováváte?

- Osobní údaje (OÚ)
- Zvláštní kategorie osobních údajů (citlivé OÚ)

AUTOCONT

Co to vlastně je „osobní údaj“ (OÚ)?

Dle GDPR:	Dle zákona č. 101/2000 Sb.:
- informace o identifikované nebo identifikovatelné fyzické osobě, - lze přímo či nepřímo identifikovat na základě jména, identifikačního čísla, lokačních údajů, prvků fyzické, fyziologické (biometrické), genetické, psychické, ekonomické, kulturní nebo společenské identity, e-mail, on-line identifikátorů (IP adresa) nebo cookies	- informace týkající se určeného nebo určitelného subjektu údajů - lze přímo či nepřímo identifikovat zejména na základě čísla, kódu nebo jednoho či více prvků, specifických pro jeho fyzickou, fyziologickou, psychickou, ekonomickou, kulturní nebo sociální identitu

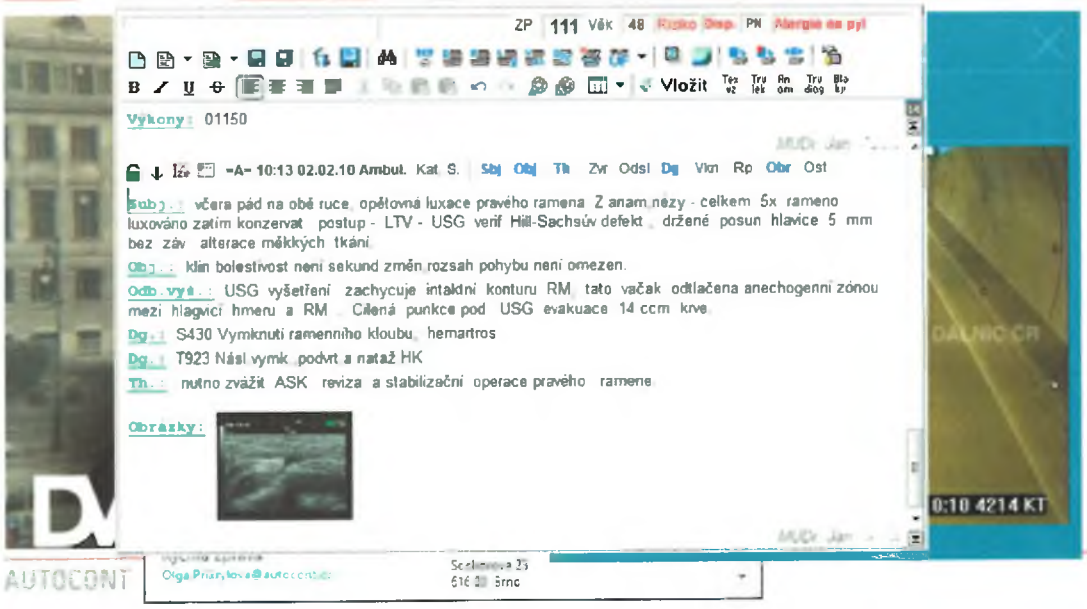
AUTOCONT

Co to je „citlivý údaj“?

Dle GDPR:	Dle zákona č. 101/2000 Sb.:
Zvláštní kategorie osobních údajů - např. o zdravotním stavu - podrobnější právní úprava ponechána na členských zemích	- o národnostním, rasovém nebo etnickém původu, - politických postojích, členství v odborových organizacích, - náboženství a filozofickém přesvědčení, - odsouzení za trestný čin, - zdravotním stavu (tělesném a duševním, vč. lék. záznamů) a sexuálním životě, - genetický a biometrický údaj umožňující přímou identifikaci nebo autentizaci SÚ

AUTOCONT

Kontrolní otázka: poznáte osobní/citlivé údaje?



Co znamená zkratka „GDPR“?

- Nařízení 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
- Nařízení X směrnice

GDPR - od kdy platí?

- Nařízení nabývá účinnosti již **25. května 2018**
- Správce (a zpracovatel) má cca **1 rok** na zavedení všech „povinných opatření"
- K datu účinnosti musí správci/zpracovatelé splňovat požadavky GDPR (přinejmenším v rozsahu, který je pro ně závazný)
- K datu účinnosti mohou být správcům/zpracovatelům OÚ uděleny sankce

AUTOCONT

GDPR - co hrozí?

Při nedodržení nebo porušení požadavků GDPR sankce

- až do: **20 000 000 Euro (540 000 000 Kč)**
- nebo **4 %**

z ročního (celosvětového) **obratu** firmy

- *Pro srovnání:*
  - *dosavadní pokuty ÚOOÚ mohou dosáhnout max. 10 miliónů (Kč)*

AUTOCONT

GDPR - pro koho platí?

- Kdokoliv (i mimo EU), kdo zpracovává nebo shromažďuje OÚ občanů členských zemí EU
  - veřejný sektor
  - soukromý sektor, **zejména** pokud zpracování OÚ souvisí:
    - s nabídkou zboží nebo služeb
    - s monitorováním chování fyzických osob
- Výjimky:
  - zpravodajské služby
  - policie
  - apod.
- Nařízení prakticky stírá rozdíl mezi správcem a zpracovatelem!

AUTOCONT

Jste správcem nebo zpracovatelem?

- **Správce**:
  - osoba (práv.) určující účel a prostředky zpracování OÚ
  - osoba (práv.) zodpovědná za jejich ochranu

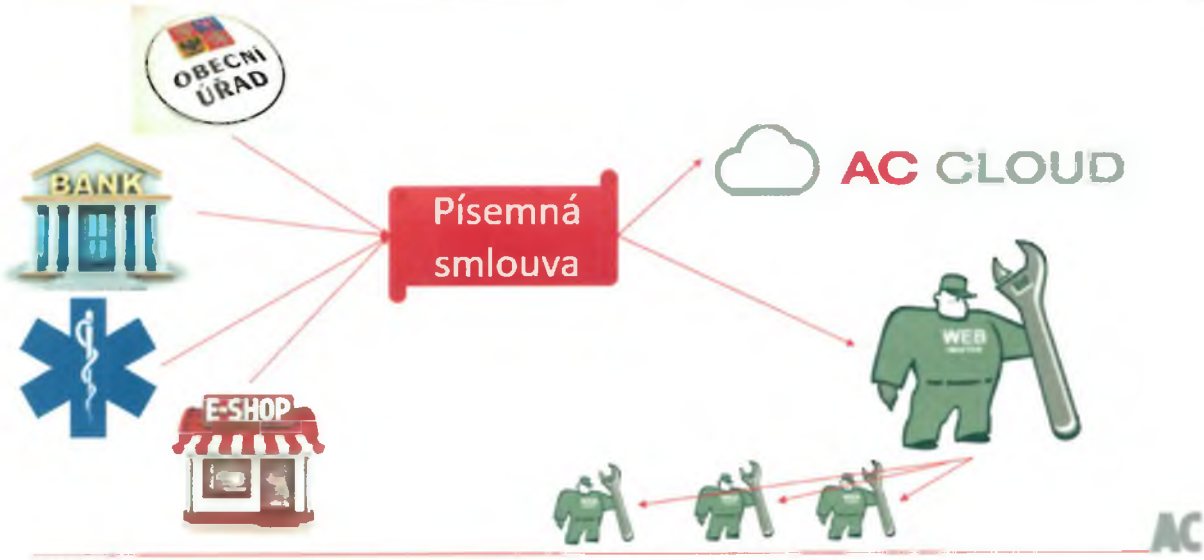
  Např.: obchodní firma s vlastním e-shopem, zdravotnické zařízení, obecní úřad.
- **Zpracovatel**:
  - osoba (práv.) pověřená správcem zpracovávat OÚ
  - nově stejná odpovědnost jako správce
  - nově ustanovena povinná písemná smlouva mezi správcem a zpracovatelem

  Např.: dodavatelská firma provozující pro obchodní firmu e-shop, informační systém, cloudové služby, outsourcing, zpracování mezd (jakékoliv služby, při nichž dochází ke zpracování OÚ)

Na velikosti nezáleží!!!

AUTOCONT

Správce vs. zpracovatel



AUTOCONT

Povinnosti správců/zpracovatelů

- Odpovědnost
- Smluvní vztahy
- Původ OÚ
- Účel/y zpracování
  - test kompatibility
- Minimalizace
- Omezení doby zpracování
- Pseudonymizace
- DPO
- Vedení záznamů
- Hlášení incidentů
- Hodnocení vlivu
- Zákonnost
- Zabezpečení
- Přenositelnost

AUTOCONT

Co nařízení nařizuje správci i zpracovateli?

15

- Musí být schopen prokázat, co je v jeho případě „odpovídající" prostředek na základě analýzy rizik!

AUTOCONT

Povinnosti vůči subjektům údajů

16

OÚ = majetek fyzické osoby

- Bezplatnost (výjimky)
- Informovanost o opatřeních
- Srozumitelné informace:
  - rozsah
  - místa uložení/zpracování
  - doba zpracování
  - příjemci
  - třetí strany
  - zabezpečení
- Hlášení incidentů

- Zajištění práv SÚ:
  - právo na přístup k OÚ
  - požadavek na opravu/úpravu
  - omezení zpracování
  - vznesení námitky (= zvláštní režim pro OÚ)
  - nesouhlas se zpracováním
  - výmaz (právo být zapomenut)
  - přenositelnost

  + povinnost informovat o požadavku SÚ další správce/zpracovatele

AUTOCONT

Povinnosti vůči ÚOOÚ

úřad pro ochranu osobních údajů

- **Záznamy** „o činnostech zpracování OÚ“
- Hlášení incidentů (do 72 hodin)
- „Odpovídající“ opatření
- Analýza rizik OÚ
- Posouzení vlivu
- Komunikace s ÚOOÚ (schválení kodexu, závazných pravidel apod.)

Kdy je zpracování OÚ zákonné?

Pouze pokud je splněna nejméně jedna z těchto podmínek a pouze v odpovídajícím rozsahu:

- **subjekt** OÚ **udělil souhlas**
- **zpracování** OÚ **je nezbytné** pro:
  - splnění smlouvy
  - splnění právní povinnosti
  - ochranu životně důležitých zájmů subjektu OÚ nebo jiné fyzické osoby
  - splnění úkolu ve veřejném zájmu nebo při výkonu veřejné moci
  - účely oprávněných zájmů
    (netýká se zpracování prováděného OVM při plnění jejich úkolů)

Souhlas

Schopnost správce (nebo zpracovatele) vždy:

- doložit, že subjekt údajů udělil souhlas se zpracováním
- získat a po celou dobu zpracování uchovávat průkazný souhlas se zpracováním

Souhlas musí být:

- svobodný
- určitý
- informovaný
- srozumitelný
- jednoznačný

AUTOCONT

ÚOOÚ a oblasti „zákonného“ zpracování OÚ

- výčet zákonných agend a s nimi souvisejících postupů týkajících se zpracování OÚ

Oblasti zpracování osobních údajů

Ústavní zakotvení ochrany osobních údajů, právo na ochranu soukromí	Pojišťovnictví
Archivnictví	Policejní postupy, veřejný pořádek, vnitřní a vnější bezpečnost
Bankovnictví, finance	Poskytování informací veřejnou správou, veřejné rejstříky a evidence
Daňové řízení	Pracovněprávní vztahy, zaměstnanost
Doprava	Předávání osobních údajů do zahraničí
Elektronická veřejná správa (e-government)	Rodná čísla
Elektronické komunikace	Rozhlasové a televizní poplatky
Evidence obyvatel, matriky a notáři	Sociální zabezpečení
Kamerové systémy	Statistická zjišťování
Kasina	Školství
Katastr nemovitostí	Územní samospráva
Nevyžádaná obchodní sdělení	Volby
Osobní doklady	Zdravotnictví

AUTOCONT

Novinka

- Nařízení zavádí (a v konkrétních případech vyžaduje) novou roli:

DPO

Data Protection Officer

(pověřenec pro ochranu OÚ)

Kdy musí být jmenován DPO?

Správce a zpracovatel jmenují pověřence pro ochranu OÚ vždy, když:

- zpracování provádí OVM či veřejný subjekt
  (s výjimkou soudů jednajících v rámci svých soudních pravomocí)
- hlavní činností správce nebo zpracovatele je:
  - rozsáhlé pravidelné a systematické monitorování subjektů údajů
  - rozsáhlé zpracování zvláštních kategorií údajů
  - rozsáhlé zpracování OÚ týkajících se rozsudků v trestních věcech a trestných činů

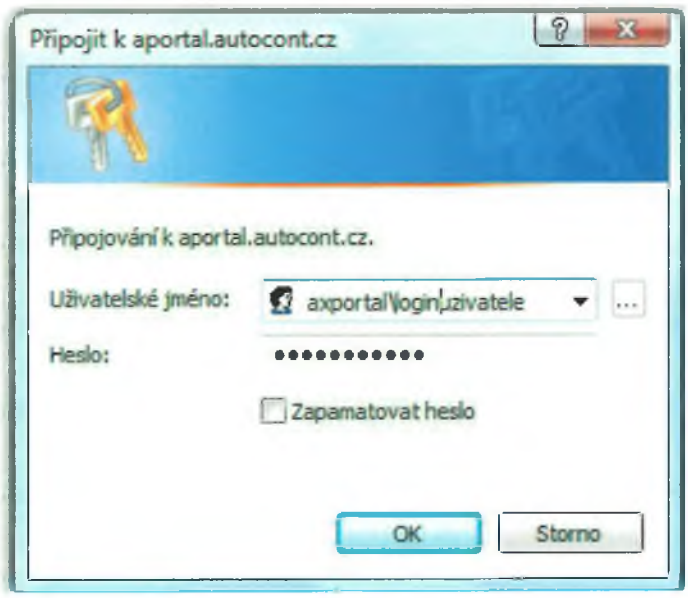
8.3 Příloha č.3 - Popis helpdeskového systému

Aportal – web pro přístup k servisním smlouvám

1. Přihlášení do systému

https://aportal.autocont.cz/weby/AUTOCONT

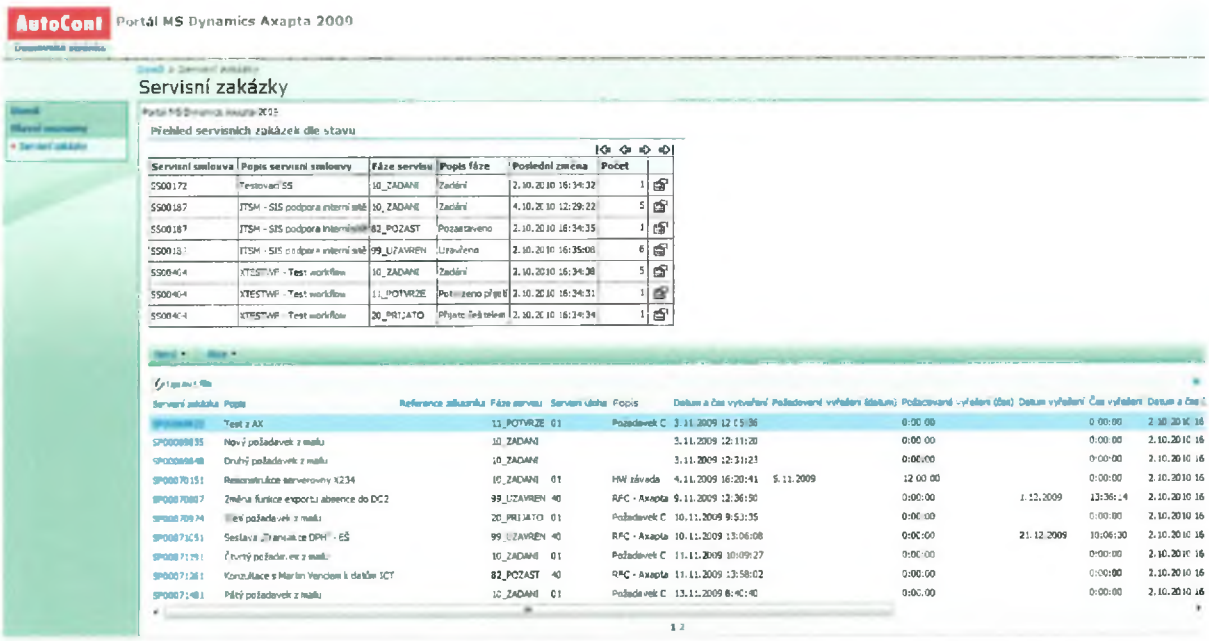
Login je potřeba zadat včetně axportal\loginuzivatele



2. Modul Servis

Po přihlášení se automaticky otevře stránka se servisními zakázkami.
(Pokud se náhodou stránka nezobrazí, klikněte prosím na záložku Domovská stránka)

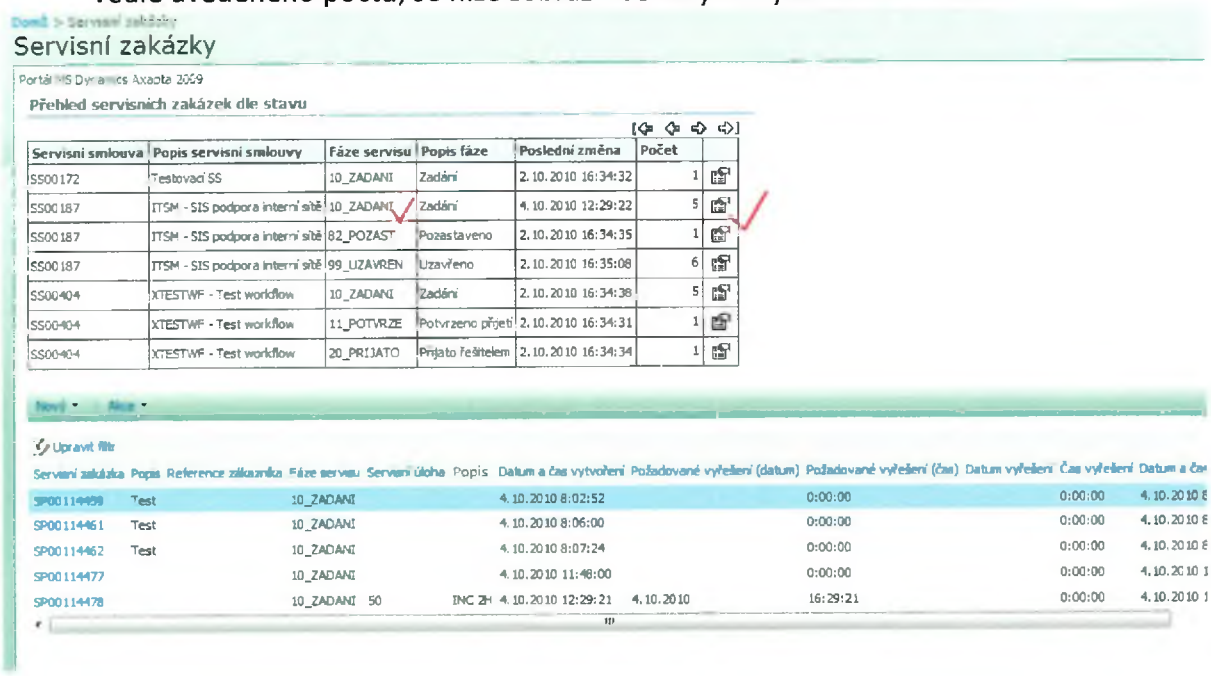
V hlavním okně je pak zobrazen **Přehled servisních zakázek dle fáze servisu**. Pod ním pak seznam všech SZ.



3. Modul Servis – základní popis

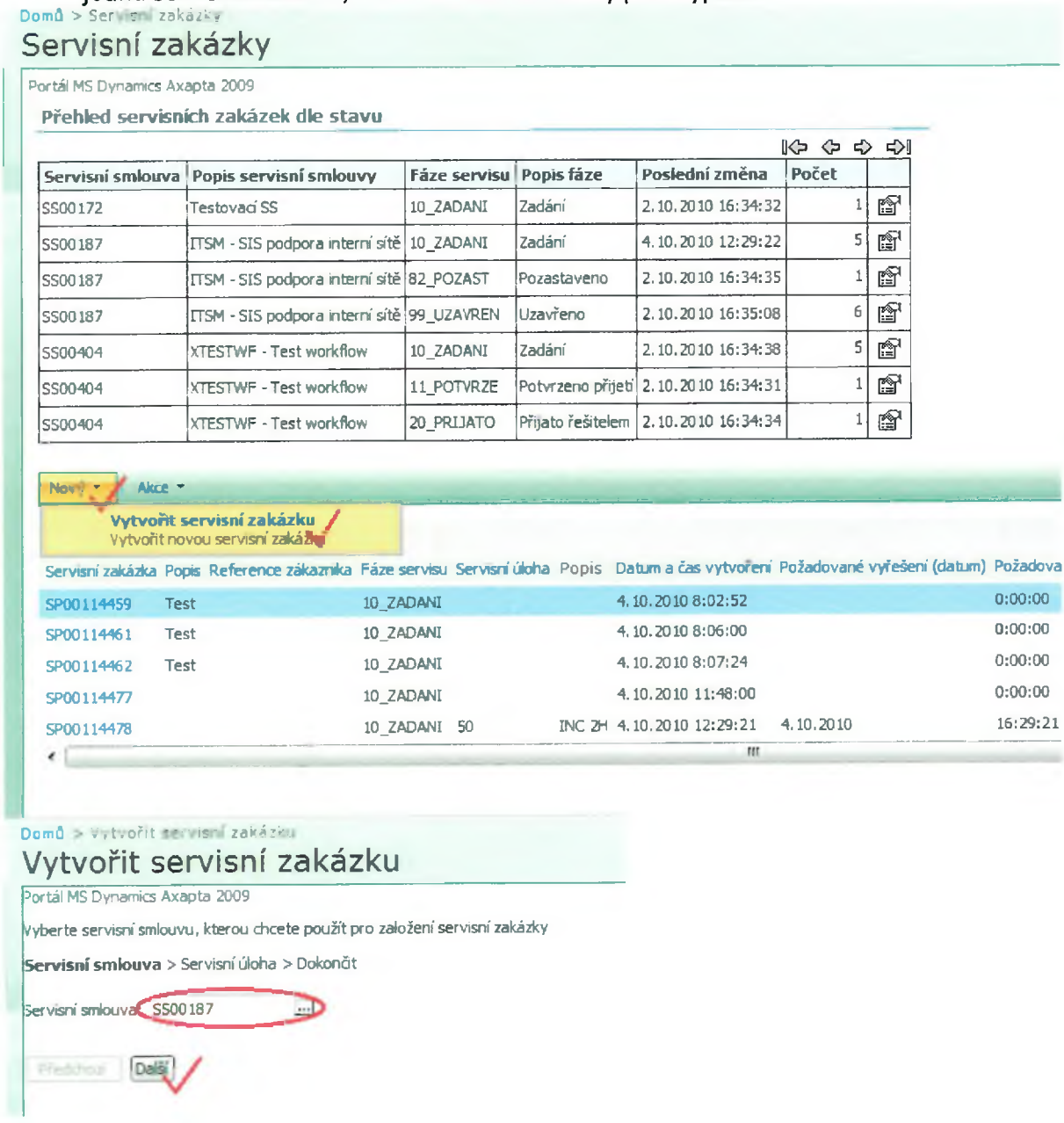
Přehled servisních zakázek dle stavu zobrazuje seznam servisních zakázek (dále jen SZ) seskupených podle Servisní smlouvy (dále jen SS) a fáze servisní zakázky.

Sloupec **Počet** zobrazuje množství SZ na dané SS a v dané Fázi. Po kliknutí na symbol vedle uvedeného počtu, se níže zobrazí všechny SZ vybrané SS a Fáze.

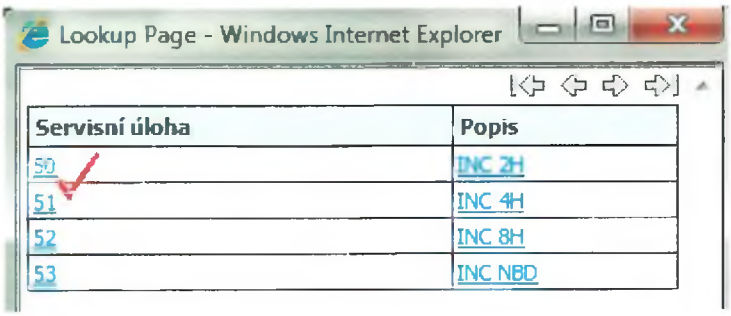


4. Vytvoření nové SZ

Klikněte na **Vytvořit servisní zakázku** a následně vyberte číslo SS. Pokud má zákazník jen jednu servisní smlouvu, číslo SS se automaticky předvyplní.



Servisní smlouvu vyberete kliknutím na ikonu ... a výběrem řádku se zvolenou Servisní úlohou. Jde o službu dle smlouvy, kterou může zákazník požadovat.
Pozn.: Tento krok se nemusí zobrazit vždy. Závisí na charakteru servisní smlouvy.



Pokračujte kliknutím na tlačítko **Další**

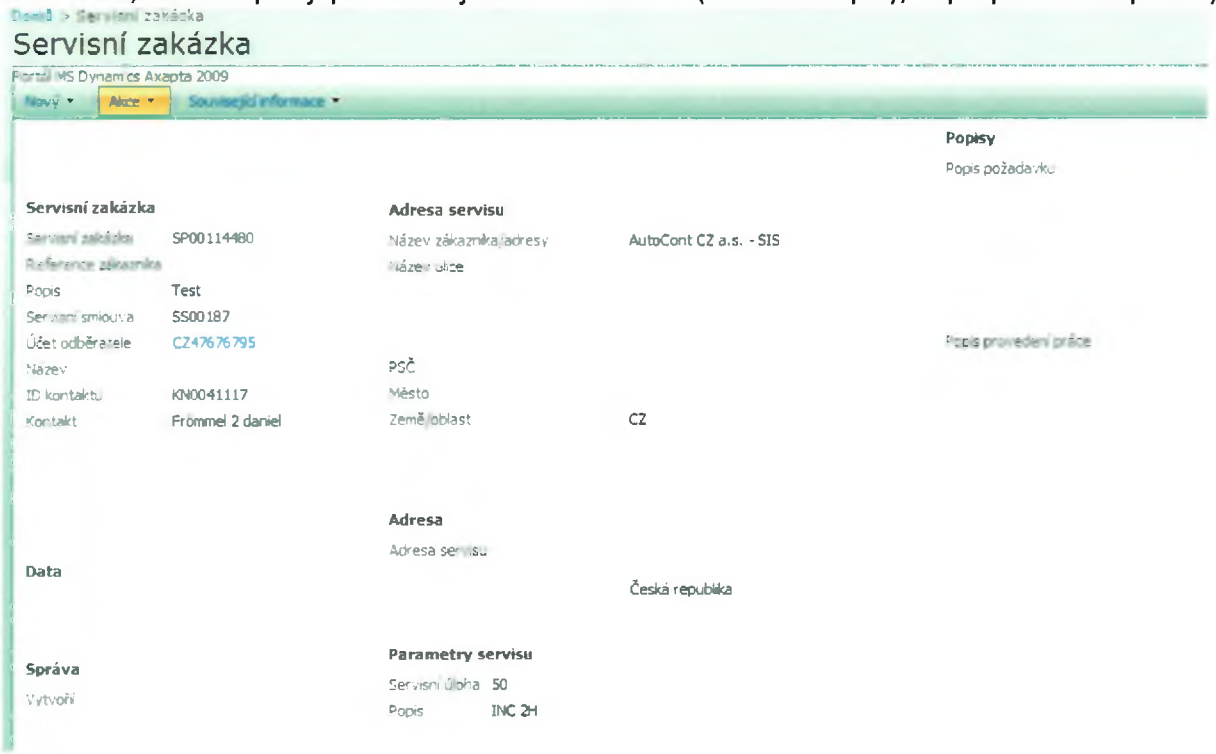
Doplňte další údaje k SZ – Popisy, Kontakty, případně referenci.

Kliknutím na tlačítko **Dokončit** vytvoříte novou SZ a zobrazí se její detail.

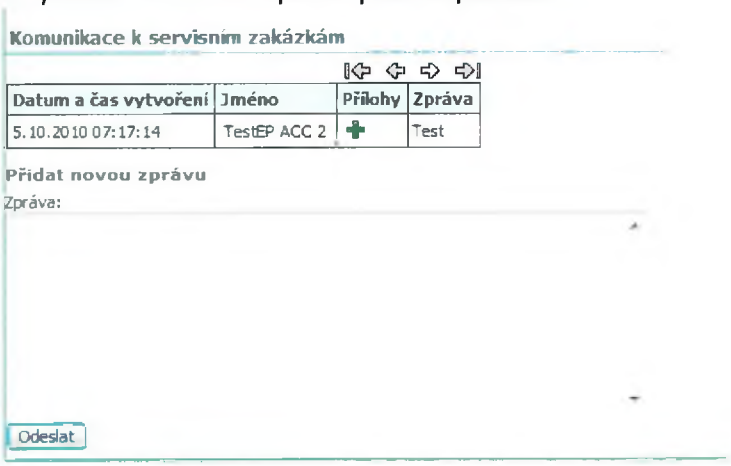
5. Detail SZ

Detail SZ se zobrazí po dokončení průvodce založením nové SZ, nebo kliknutím na číslo SZ v přehledu SZ.

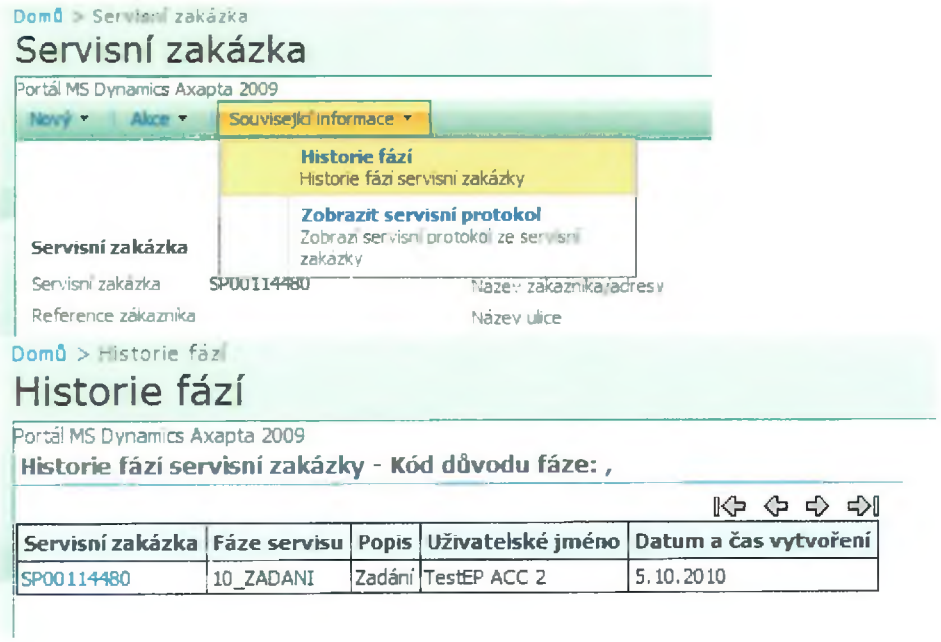
V detailu SZ se zobrazí:
Popis SZ – v jednotlivých záložkách najdete informace o SZ, které jste zadali při zadání SZ, případně informace, které dopisují při řešení jednotliví technici (Záložka Popisy/Popis provedení práce)



Komunikace k servisním zakázkám – jde o „chat", kde lze navázat komunikaci mezi zákazníkem a servisním střediskem. Zprávu zapište do dialogového okna **Zpráva** a odešlete ji tlačítkem **Odeslat**. Kliknutím na symbol ✚ lze ke zprávě přiložit přílohu.

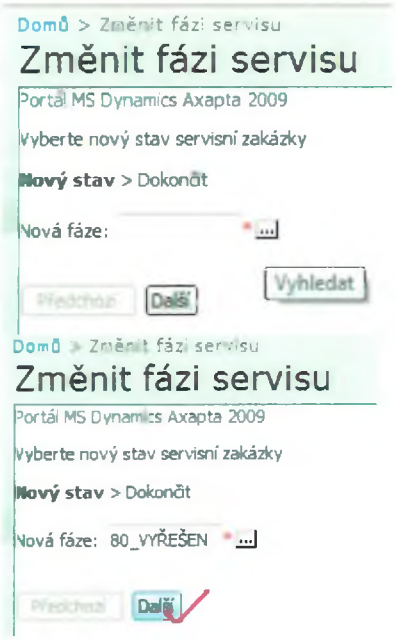


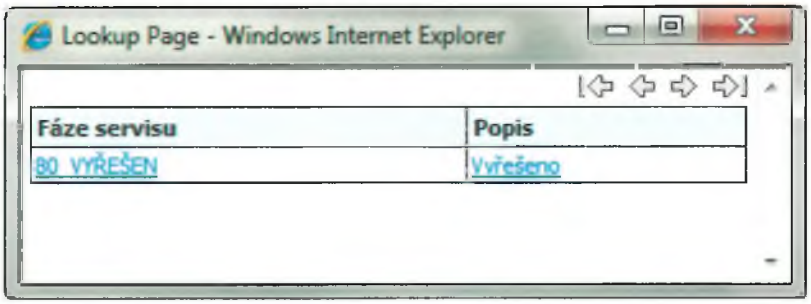
Historie fází servisní zakázky – záznam změny stavů dané SZ



6. Posunutí fáze SZ

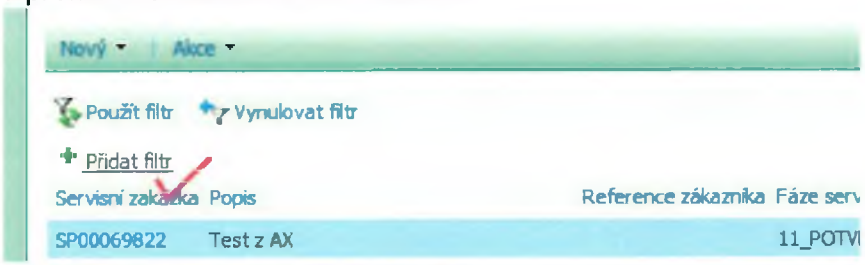
Týká se jen servisních smluv, kde je tato interakce se zákazníkem nastavena.



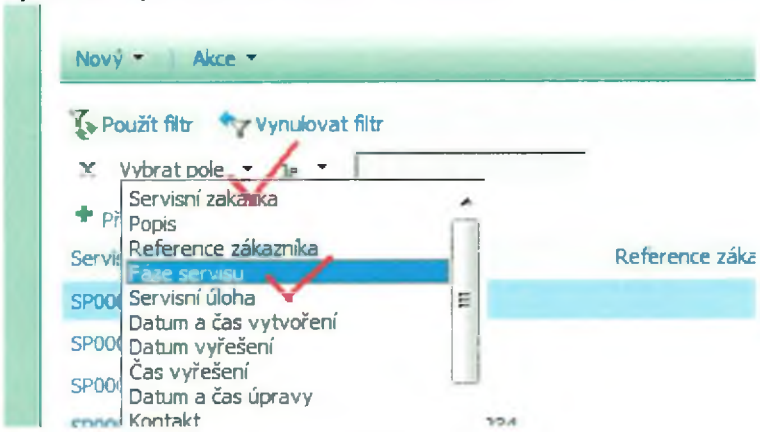


7. Filtrování SZ

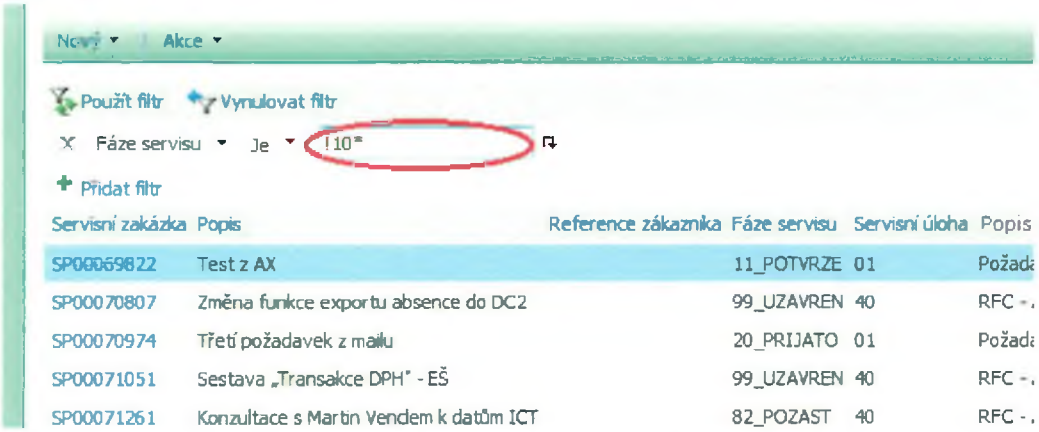
V přeheldu SZ klikneme na Přidat filtr



Vybereme pole, které chceme filtrovat



Nastavíme podmínku a potvrdíme. Syntaxe pro vytvoření podmínky jsou uvedeny níže.



Tímto způsobem můžeme do filtru přidat další pole Přidat filtr

Nastavený filtr vynulujeme pomoci Vynulovat filtr

Syntaxe-nejpoužívanější tvary filtrů

Syntaxe	Popis znaku	Popis	Příklad
hodnota	Rovno zadané hodnotě.	Zadejte hodnotu, kterou chcete vyhledat.	Smith vyhledá "Smith".
!hodnota **(vykřičník)**	Není rovno zadané hodnotě.	Před hodnotu, kterou chcete vyloučit, zadejte vykřičník.	!Smith vyhledá všechny hodnoty kromě hodnoty "Smith".
Od hodnota..Do hodnota **(dvě tečky)**	Mezi dvěma zadanými hodnotami oddělenými dvěma tečkami.	Zadejte hodnotu Od, pak dvě tečky a nakonec hodnotu Do.	1..10 vyhledá všechny hodnoty od 1 do 10. Avšak v poli řetězců A..C vyhledá všechny hodnoty začínající na "A" a "B" a hodnoty přesně rovny "C" (například "Ca" nebude nalezena). Chcete-li vyhledat všechny hodnoty od "A*" do "C*", napište A..D.
..hodnota **(dvě tečky)**	Méně nebo rovno zadané hodnotě.	Zadejte dvě tečky a pak hodnotu.	..1000 vyhledá libovolné číslo menší nebo rovné hodnotě 1000: například "100", "999,95" a 1.000.
hodnota.. **(dvě tečky)**	Větší nebo rovno zadané hodnotě.	Zadejte hodnotu a pak dvě tečky.	Hodnota 1000.. vyhledá číslo větší nebo rovno hodnotě 1000: například "1.000", "1.000,01" a "1.000.000".
>hodnota **(větší než)**	Větší než zadaná hodnota.	Zadejte znaménko "větší než" a pak hodnotu.	>1000 nalezne libovolné číslo větší než 1000: například "1.000,01", "20.000" a "1.000.000".
<hodnota **(menší než)**	Menší než zadaná hodnota.	Zadejte znaménko "menší než" a pak hodnotu.	<1000 nalezne libovolné číslo menší než 1000: například "999,99", "1" a "-200".
hodnota* **(hvězdička)**	Začít zadanou hodnotou.	Zadejte počáteční hodnotu a pak hvězdičku.	S* nalezne libovolný řetězec začínající na S, jako například "Stockholm", "Sydney" nebo "San Francisco."
****hodnota*** **(hvězdička)**	Skončit zadanou hodnotou.	Zadejte hvězdičku a pak konečnou hodnotu.	*východ nalezne řetězec končící na "východ", jako například "severovýchod" nebo "jihovýchod."
****hodnota**** **(hvězdička)**	Obsahuje zadanou hodnotu.	Zadejte hvězdičku, pak hodnotu, a nakonec opět hvězdičku.	*ch* nalezne libovolný řetězec obsahující "ch", jako například "severovýchod" nebo "jihovýchod."

8.4 Příloha č.4 – Subdodavatelská smlouva

SMLOUVA

uzavřená dle ustanovení § 1746/2 Občanského zákoníku v platném znění

Článek 1

Smluvní strany

Společnost: **AutoCont CZ a.s.**

se sídlem: 702 00 Ostrava – Moravská Ostrava, Hornopolní 3322/34
zastoupena: Ing. Zdeněk Chobot, ředitel regionálního centra, na základě plné moci
IČ: 47676795
DIČ: CZ47676795
Bankovní spojení: Česká spořitelna a.s., [redacted]

Společnost je zapsaná v obchodním rejstříku vedeném u Krajského soudu v Ostravě, oddíl B, vložka 814

dále též "**dodavatel**"

a

Společnost: **ELSO s.r.o.**

se sídlem: Politických vězňů 911/8, Nové Město, 110 00 Praha 1
zastoupena: Ing. Martin Kubeš
IČ: 60487721
DIČ: CZ60487721
Bankovní spojení: Fio banka a.s., č.ú.: [redacted]

Společnost je zapsaná v obchodním rejstříku vedeném u Městského soudu v Praze pod značkou C 27229

dále též "**poddodavatel**"

Článek 2

Předmět smlouvy

1. Smlouva je uzavírána za účelem zajištění plnění v případě získání veřejné zakázky „**Kybernetická bezpečnost**" vypsané Statutárním městem Karlovy Vary (dále jen „Veřejná zakázka"), a to v rozsahu služeb v oblasti síťové infrastruktury.
2. Smluvní strany se dohodly, že ve Veřejné zakázce podle odstavce 2.1. bude společnost AutoCont CZ a.s. vystupovat jako dodavatel; společnost ELSO s.r.o. bude poddodavatelem, přičemž jako poddodavatel souhlasí s tím, aby byla uvedena v nabídce dodavatele.
3. Pro případ, že nabídka dodavatele bude ve Veřejné zakázce vyhodnocena jako ekonomicky nejvýhodnější a dodavatel uzavře smlouvu se zadavatelem, zavazuje se poddodavatel k poskytnutí plnění určeného k plnění Veřejné zakázky dodavatelem či k poskytnutí věcí či práv, s nimiž bude dodavatel oprávněn disponovat v rámci plnění Veřejné zakázky.
4. Poddodavatel nese společnou a nerozdílnou odpovědnost za plnění Veřejné zakázky společně s dodavatelem.
5. Poddodavatel se zavazuje, že bude vykonávat práce či služby rozsahu odstavce 2.1. Poddodavatel je připraven využít a poskytnout ve prospěch dodavatele ve Veřejné zakázce

v rozsahu poddodávky svou kapacitu. Poddodavatel se zavazuje, že vyvine veškeré úsilí a poskytne maximální podporu dodavateli při případné realizaci Veřejné zakázky. Dodavatel bude při plnění předmětu Veřejné zakázky oprávněn disponovat plněním poskytnutým poddodavatelem, v rozsahu nezbytném k řádnému plnění Veřejné zakázky.

6. Poddodavatel se bude při plnění dodávky podílet zejména na implementaci síťové infrastruktury LAN.

Článek 3

Společná ustanovení

1. Smluvní vztah založený touto smlouvou se uzavírá na dobu plnění závazků vyplývajících z Veřejné zakázky a skončí splněním všech závazků z Veřejné zakázky vyplývajících.
2. Obě smluvní strany potvrzují, že tato smlouva byla uzavřena svobodně a vážně, na základě projevené vůle obou smluvních stran, že souhlasí s jejím obsahem, a že tato smlouva nebyla ujednána za jednostranně nevýhodných podmínek.
3. Tato smlouva nabývá platnosti a účinnosti dnem jejího podpisu oběma smluvními stranami.
4. Smlouva se vyhotovuje ve třech stejnopisech, z nichž každá smluvní strana obdrží po jednom vyhotovení a jedno vyhotovení se předkládá zadavateli Veřejné zakázky.

V Praze, dne 9.1.2018

Poddodavatel
ELSO s.r.o.

[redacted]

.....
Martin Kubeš
jednatel společnosti

[redacted]

V Karlových Varech, dne 10. 1. 2018

Dodavatel
AutoCont CZ a.s.

[redacted]

.....
Zdeněk Chobot,
ředitel regionálního centra,
na základě plné moci