# **Sdílený email Kraje Vysočina – technické zadání**

**Specifikace předmětu zakázky:** Vytvoření služby (SaaS) sdíleného emailového serveru s groupwarovými službami v multitenantních architektuře v prostředí on-premise v rámci Technologického centra Kraje Vysočina (virtualizace na platformě VMWare ESX).

**Všeobecné požadavky:**

1. Vytvořit pro zadavatele emailový server s groupwarovými službami splňující technické požadavky dle technické specifikace a poskytnout zadavateli potřebné licence pro požadované funkcionality P1 a P2 (viz níže) i nabízených funkcionalit R, a podporu k tomuto dílu.
2. Provést kompletní instalaci a implementaci do prostředí zadavatele (Technologické centrum Kraje Vysočina), tj. do prostředí serverové virtualizace (VMware ESX) typicky na serverové platformě MS Windows 2016. Maximální výkon alokovaný z fyzických hostů všemi virtuálními stroji (max. 4 kusy VM, libovolný OS podporovaný VMWarem) je 4 GHz CPU, max. spotřeba paměti je 32 GB RAM. K dispozici jsou mechanismy vysoké dostupnosti (HA režim VMW), síťové ochrany včetně Web Application Firewallu (F5 BIG IP) a zálohování je zajištěno nativními nástroji použité serverové virtualizace, systémem Veeam. Licence OS Microsoft Windows Server Datacenter a sdíleného MS SQL 2016 Standard serveru jsou zajištěny zadavatelem.
3. Poskytnout technické zaškolení administrátory
4. Poskytovat technickou podporu pro dílo.

Zadavatel má právo vyzvat účastníka řízení, který podal nabídku, k prezentaci nabízeného řešení u vybraných požadavků typu P1.

# **Email server s groupware – technická specifikace**

**Typy požadavků:**

P1 – technický požadavek, který musí řešení uchazeče splňovat v době podání nabídky. Zadavatel může požadovat ukázku naplnění funkcionality.

P2 - technický požadavek, který musí řešení uchazeče splňovat v době ukončení implementace díla

R - rozšiřující technický požadavek, nepovinný. Viz kritérium 2 hodnocení.

|  |  |  |
| --- | --- | --- |
| **ID** | **Popis** | **Povinné (P1,P2) / rozšiřující (R)** |
| EML01 | Licence pro 400 uživatelů a zařízení a neomezený počet organizací (tenatů) – pokud licenční model neumožňuje toto licencování, za neomezený počet je považováno 200 organizací. Kusová cena této licence je platná i pro nákup dalších licencí nad rámec 400ks. | P1 |
| EML02 | Možnost rozšíření licence na neomezený počet uživatelů, zařízení a organizací pro všechny moduly. V případě, že licenční model neumožňuje toto licencování, je za neomezený počet považováno 4000 uživatelů, 4000 zařízení a 200 organizací. | P1 |
| EML03 | Dostupnost služeb z veřejných i privátních sítí přes standardní emailové protokoly – IMAP, SMTP, POP3 včetně jejich šifrovaných verzí | P1 |
| EML04 | Technologie ActiveSync pro komunikaci s mobilními klienty. Licence pro všechny klienty. | P1 |
| EML05 | Připojení klientů mobilních platforem Android i iOS | P1 |
| EML06 | Synchronizace adresáře (CarDAV) s mobilními zařízeními s OS Android a iOS | P2 |
| EML07 | Synchronizace kalendáře (CalDAV) s mobilními zařízeními s OS Android a iOS | P2 |
| EML08 | Kompatibilita s MS Outlook 2016 a novější včetně funkcí synchronizace emailu, kalendáře, úkolů a fultextového vyhledávání v těchto položkách. Licence (synchronizace, nikoliv samotného produktu MS Outlook) pro všechny klienty. | P1 |
| EML09 | Webový klient umožňující plnohodnotný bezpečný přístup k poštovní schránce bez nutnosti instalace doplňků do prohlížeče a OS | P1 |
| EML10 | Šifrování a el. podepisování zpráv prostřednictvím PKI (S-MIME) na úrovni desktopového klienta. Šifrování a el. podepisování musí být možné promocí kvalifikovaného el. prostředku (kval. el. podpis dle eidas) např. karta. | P1 |
| EML11 | Šifrování a el. podepisování zpráv prostřednictvím PKI (S-MIME) na úrovni webového klienta Šifrování a el. podepisování musí být možné promocí kvalifikovaného el. prostředku (kval. el. podpis dle eidas) např. karta. | P2 |
| EML12 | Podpora autentizace k webovému klientovi prostřednictvím SSO Kraje Vysočina (SAML2) federace VysočinaID viz https://vysocinaid.kr-vysocina.cz/ | P2 |
| EML13 | Podpora dvoufaktorové autentizace (Google Authenticator, U2F /FIDO2 standard/, popř. SMS OTP) pro přístup k webovému klientu | P2 |
| EML14 | Podpora dvoufaktorové autentizace ActiveSync | R |
| EML15 | Autorizace IDM – synchronizace informací o uživatelích, rolí a organizační struktuře z IDM Kraje Vysočina (AC Identita) | P2 |
| EML16 | Plná provozovatelnost v uzavřené síti (ROWANet) bez dostupnosti veřejného internetu | P2 |
| EML17 | Podpora technologie maillistu včetně webového rozhraní pro správu a registraci | P2 |
| EML18 | Provoz 16-ti domén (DNS/MX) a to i v jedné organizaci (tenantu) | P2 |
| EML19 | Možnost definice politik objemových kvót mailboxů s možností více politik per tenant | P2 |
| EML20 | Řešení antispamové a antivirové ochrany | P2 |
| EML21 | Podpora služeb adresářů globálních (přes všechny tenanty) a lokálních (v daném tenantu) | P2 |
| EML22 | Služby kalendáře a plánování včetně sdílení a nahlížení do kalendářů (s možností nastavení oprávnění) v tenantu i přes vybrané tenanty | P2 |
| EML23 | Nástroj pro hromadný import zpráv z formátu EML, MSG a PST | P2 |
| EML24 | Nástroj pro hromadný export zpráv do formátu EML a MSG  | P2 |
| EML25 | Nástroj pro hromadný export zpráv do formátu PST | R |
| EML26 | Řešení pro centrální archivaci nepoužívaných emailů mimo hlavní mailbox klienta s možností fulltextového vyhledávání | R |
| EML27 | Nástroje týmové práce: skupinový a individuální chat | R |
| EML28 | Nástroje týmové práce: skupinová a individuální videokonference | R |
| EML29 | Nástroje týmové práce: skupinové a individuální úložiště dokumentů | R |
| EML30 | Granulární obnova jednotlivých emailů nástrojem VEEAM BACKUP and REPLICATION | R |
| EML31 | Nastavení mail flow a max. velikosti zpráv na mail konektoru per tenant včetně nastavení oprávnění | P2 |
| EML32 | Bezpečnost: Logování a auditní záznamy – systém musí splňovat požadavky na logování a auditní záznamy uvedené v této specifikaci níže v kapitole Bezpečnostní specifikace.  | P2 |
| EML33 | Bezpečnost: Aplikační servery/moduly (např. web server, DB server, apod.) nesmí vyžadovat pro své spuštění privilegovaná oprávnění (např. typu root, Administrator, NT Authority\System, apod.) | P2 |
| EML34 | Bezpečnost: Přenos dat musí probíhat vždy pomocí zabezpečeného protokolu, např. HTTPS, SMTPS, IMAPS, LDAP over TLS (STARTLS nebo LDAPS), …  | P2 |
| EML35 | Bezpečnost: Systém musí umožňovat přenos dat do sítě Internet přes aplikační HTTP proxy, která je systémově nastavená (případně lze konfigurovat přímo v aplikaci).  | P2 |
| EML36 | Bezpečnost: Dodavatel musí při implementaci systému vyspecifikovat všechny potřebné zdroje z internetu, které jsou nezbytné pro provoz systému za účelem vytvoření tzv. white-listu na aplikační HTTP proxy.  | P2 |
| EML37 | Bezpečnost: Systém a jeho implementace musí naplňovat požadavky na kryptografii uvedené v této specifikaci níže v kapitole Bezpečnostní specifikace u těch bodů, které jsou pro daný systém relevantní. | P2 |
| EML38 | Bezpečnost: Dodavatel musí při implementaci zpracovat analýzu rizik provozu systému tak, jak je uvedené v této specifikaci níže v kapitole Bezpečnostní specifikace.  | P2 |
| EML39 | Bezpečnost: Provozně-bezpečnostní dokumentace – dodavatel musí při implementaci zpracovat provozně-bezpečnostní dokumentaci a to minimálně v rozsahu uvedeném v této specifikaci níže v kapitole Bezpečnostní specifikace.  | P2 |
| EML40 | Nástroj pro administraci jednotlivých tenantů ze strany administrátora tenantu (organizace) minimálně v rozsahu správy mailboxů a exportu dat. | P2 |

# **Bezpečnostní specifikace**

## Logování a auditní záznamy

Auditní záznamy a logy musí obsahovat minimálně tyto informace:

* přihlášení a odhlášení všech uživatelů (včetně administrátorů či jiných privilegovaných účtů),
* činnosti provedené administrátory, např. (pokud danou funkcionalitu obsahují):
	+ přidělení/odebrání oprávnění,
	+ založení/smazání uživatele či mailboxu,
	+ přidělení/odebrání role,
	+ reset hesla (pokud je prováděn na úrovni systému),
	+ povýšení oprávnění administrátora, převzetí role konkrétního uživatele,
	+ nahlížení do mailboxu cizího uživatele,
	+ změna konfigurace logování událostí,
	+ změna konfigurace informačního aktiva,
* činnosti prováděné uživateli,
* automatická informační, varovná a chybová hlášení provozního charakteru (tzv. provozní aplikační logy).

Auditní záznamy a logy musí obsahovat minimálně tyto parametry a metadata:

* identifikátor události,
* identifikátor zdroje událostí včetně toho původního (v případě použití proxy prvků v síti, je nutné logovat i původní zdroj událostí, např. z http header X-Forwarded-To),
* přesné datum vzniku události,
* přesný čas vzniku události včetně specifikace časového pásma,
* typ/název události,
* případně popis události (pokud není zřejmé z typu/názvu nebo není uvedeno v dokumentaci),
* jednoznačnou identifikaci účtu, pod kterým byla událost provedena,
* jednoznačnou síťovou identifikaci zařízení původce (včetně původního zdroje v případě použití proxy prvků v síti) a
* úspěšnost nebo neúspěšnost (včetně neprovedení činnosti v důsledku nedostatečných oprávnění) události.

Formát (resp. standard) logů musí být v jedné z následujících možností:

* syslog (RFC 5424) + syslog over TLS,
* MS Windows Event Log (vlastní umístění XPath pro informační aktivum),
* W3C,
* Standardní apache web server logy,
* SQL view,
* MS SQL audit logy,
* jiné formáty, resp. standardy jsou možné pouze po předchozím schválení zadavatele. V tomto případě si zadavatel vyhrazuje právo na reálnou ukázku způsobu logování sytému.

Systém musí zaznamenávat auditní záznamy a logy na všech existujících úrovních – tj. na úrovni:

* operačního systému,
* aplikačního serveru/modulu aktiva (např. web server, smtp server, apod.)
* samostatné aplikace/informačního systému/služby informačního systému.

## Kryptografie

#### Obecně

Pro šifrování, elektronické podepisování a provádění otisků dat (hashování) nesmí být použity proprietární/uzavřené algoritmy, ale ty, které jsou považovány za standardy, jejich funkcionalita je všeobecně známá.

#### Hashovací funkce

##### Ukládání otisků hesel

* pro ukládání hesel uživatelů mohou být použity pouze tyto tzv. pomalé hashovací funkce:
	+ Argon2i
	+ bcrypt
	+ scrypt
	+ PBKDF2
* při hashování hesla musí být použit pseudonáhodně vygenerovaný kryptografický salt
* pro ukládání hesel nesmí být použity tzv. rychlé hashovací funkce typu MD-X, SHA-X, apod.

##### Elektronické podepisování e-mailů a dokumentů

* SHA-2 a vyšší
* délka otisku 256 bitů a vyšší

##### Ověřování integrity souborů

* SHA-2 a vyšší
* délka otisku 224 bitů a vyšší

#### Asymetrická kryptografie

##### SSL/TLS

* verze protokolu minimálně TLSv1.2 a vyšší
* konfigurace
	+ cipher suite musí být vybrána na základě serverem preferovaného pořadí
	+ vyšší priority musí mít cipher suites, které obsahují varianty asymetrických algoritmů s eliptickými křivkami, např.:
		- ECDHE musí mít vyšší prioritu než DHE
		- ECDSA musí mít vyšší prioritu než DSA
	+ všechny EXPORT cipher suites musí být zakázány
	+ algoritmy a funkce pro výměnu klíčů
		- algoritmus pro výměnu klíčů musí podporovat Perfect forward secrecy
			* tzn., že šifrovací klíč je vyměněn mezi klientem a serverem tak, aby jej nebylo možné získat se znalostí privátního klíče serveru, např. musí být použit Diffie-Hellman (DH nebo ECDH) algoritmus
			* a navíc se musí jednat o tzv. ephemeral Diffie-Hellman (DHE, ECDHE), tzn. že pro každou session je generován nový set Diffie-Hellman klíčů
		- délky klíčů:
			* pro Diffie-Hellman (DH) - 2048 bitů a více (postupně přecházet na 3072 bitů, tam kde to půjde)
			* pro Elliptic Curve Diffie-Hellman (ECDH) – 256 bitů a více
		- nesmí být použita anonymní výměna klíčů
	+ algoritmy a funkce pro autentizaci
		- minimální délky klíčů:
			* RSA - 2048 bitů (postupně přecházet na 3072 bitů, tam kde to půjde)
			* ECDSA - 256 bitů
	+ algoritmy a funkce pro symetrické šifrování
		- nesmí být použita hodnota NULL v cipher suites
		- nesmí být použity tyto šifry:
			* DES, 3DES, RC4
		- minimální délka šifrovacího klíče - 128 bitů
		- cipher suites s šiframi s větší délkou klíče musí mít větší prioritu v seznamu ciphersuites než s menší délkou klíče
	+ MAC (Message Authentication Code)
		- použití SHA funkce s minimální délkou hashe 256 bitů
		- vyšší délky otisků musí mít vyšší prioritu v cipher suites
* Certifikáty
	+ minimální délka privátního klíče
		- RSA 2048 bitů
		- ECDSA - 256 bitů
	+ hash funkce pro podpis
		- SHA-2 s minimální délkou 256 bitů

##### TLS cipher suites

* Doporučené cipher suites (v doporučeném pořadí), které naplňují výše zmíněné požadavky
* TLS1.3:

TLS\_AES\_256\_GCM\_SHA384

TLS\_CHACHA20\_POLY1305\_SHA256

TLS\_AES\_128\_GCM\_SHA256

TLS\_AES\_128\_CCM\_SHA256

* TLS1.2:

TLS\_ECDHE\_ECDSA\_WITH\_AES\_256\_GCM\_SHA384

TLS\_ECDHE\_ECDSA\_WITH\_CHACHA20\_POLY1305\_SHA256

TLS\_ECDHE\_ECDSA\_WITH\_AES\_128\_GCM\_SHA256

TLS\_ECDHE\_RSA\_WITH\_AES\_256\_GCM\_SHA384

TLS\_ECDHE\_RSA\_WITH\_CHACHA20\_POLY1305\_SHA256

TLS\_ECDHE\_RSA\_WITH\_AES\_128\_GCM\_SHA256

TLS\_DHE\_RSA\_WITH\_AES\_256\_GCM\_SHA384

TLS\_DHE\_RSA\_WITH\_AES\_128\_GCM\_SHA256

TLS\_DHE\_RSA\_WITH\_CHACHA20\_POLY1305\_SHA256

##### Šifrování, podepisování a autentizace

* týká se různých technologií PKI, PGP, S/MIME, SSH, apod.
* minimální délka klíče
	+ algoritmus DSA – 2048 bitů (postupně přecházet na 3072 bitů, tam kde to půjde)
	+ algoritmus RSA - 2048 bitů (postupně přecházet na 3072 bitů, tam kde to půjde)
	+ algoritmus ECDSA - 256 bitů
* Ověřování (např. SSH klíče)
	+ délka klíče minimálně 2048 bitů u RSA a DSA algoritmů (postupně přecházet na 3072 bitů, tam kde to půjde)
	+ délka klíče minimálně 256 bitů u algoritmů používajících eliptické křivky

#### Symetrická kryptografie

* nesmí být použity tyto šifry:
	+ DES, 3DES, RC4, Blowfish, Kasumi
* minimální délka šifrovacího klíče - 128 bitů
	+ pro šifru Chacha20 minimálně 256 bitů a se zatížením klíče menším než 256 GB
* nesmí být použity tyto módy pro ochranu integrity:
	+ HMAC-SHA1, CBC-MAC-X9.19

## Analýza rizik

Dodavatel se zavazuje k provedení podrobné a komplexní analýzy rizik informační bezpečnosti v souvislosti s provozem tohoto systému. Analýza rizik informační bezpečnosti musí být zpracována před nasazením do provozního režimu. Dodavatel vypracuje a předá objednateli:

* zdokumentovaný postup provedení analýzy rizik (metodiku, jak postupoval),
* zprávu z analýzy rizik obsahující vydefinovaná a klasifikovaná rizika, která jsou určena na základě míry dopadu, pravděpodobnosti výskytu zranitelnosti a pravděpodobnosti naplnění hrozby, a popis těchto rizik, kdy míra dopadu odpovídá hodnotě informačního aktiva spočítané jako průměr hodnot pro požadavky na dostupnost, důvěrnost a integritu aktiva,
* plán zvládání rizik s návrhy opatření na snížení míry případných rizik včetně popisu způsobu a návrhu termínu jejich nasazení.

Objednatel bude schvalovat výstupy z provedené analýzy rizik před nasazením informačního aktiva do provozního režimu formou akceptačního protokolu.

## Provozně-bezpečnostní dokumentace

V rámci implementace systému musí být dodavatelem dodána i provozní dokumentace v níže uvedených oblastech.

Níže je uveden popis provozní dokumentace a jsou popsány oblasti, které by provozní dokumentace měla pokrývat.

Cílem zpracování této dokumentace je popsat a zdokumentovat provozní postupy pro zajištění správného, bezchybného a bezpečného provozování systému.

#### Bezpečnostní specifikace systému

Cíl dokumentu: popsat a zdokumentovat veškeré bezpečnostní mechanizmy a opatření za účelem identifikace toho, jaká data jsou jakým způsobem chráněna.

Forma dokumentu: textový popis, buď dle metodiky ITSEM (Information Technology Security Evaluation Manual podle ITSEC) nebo v rozsahu minimálně dle následujících bodů:

* Soupis a popis všech funkcí prosazujících bezpečnost pro:
	+ zajištění integrity dat při jejich přenosu a uložení,
	+ zajištění důvěrnosti dat při jejich přenosu a uložení,
	+ zajištění autentizace a session managementu,
	+ zajištění ošetření, filtrování a prověřování veškerých vstupních dat,
	+ zajištění auditní stopy a logování,
	+ externí rozhraní – jak uživatelská, tak pro komunikaci s externími systémy.
* Popis těchto oblastí (pakliže jsou aplikovatelné):
	+ použité kryptografické funkce a algoritmy – popis přesné specifikace a použitých parametrů (typ funkce, délka klíče, mód šifrování, počet iterací, apod.),
	+ poloformální popis všech nestandardních algoritmů, funkcí a protokolů v oblasti bezpečnosti (např. vlastní šifrovací algoritmus, vlastní komunikační protokol, apod.),
	+ autentizační a autorizační model a mechanizmus (např. fáze autentizace, způsoby ověření, heslové politiky, protokoly, session management, ...),
	+ řízení uživatelských a privilegovaných rolí a oprávnění (včetně Access Control, Least Priviledge principy, Multi-factor autentizace, Segregation of Duties principy, Accountability principy)
		- To vše z pohledu:
			* Interních uživatelů
			* Externích uživatelů,
	+ detailní popis úrovně všech přístupových oprávnění/aplikačních rolí,
	+ způsob bezpečnostního testování systému,
	+ monitoring řešení a zaznamenávání logů a auditní stopy (viz část provozně bezpečnostní dokumentace Monitoring),
	+ způsob zajištění dostupnosti, důvěrnosti a integrity dat ve stavech jejich uložení/uchování, zpracování a přenosu,
	+ soulad s právními normami pro ochranu osobních údajů,
	+ bezpečnostní architektura infrastruktury,
	+ bezpečnostní architektura klienta/koncového zařízení,
	+ disaster recovery plán a strategie zálohování,
	+ u webových aplikací popis způsobu ošetření aplikace dle OWASP Testing guide v aktuální verzi.

#### Základní konfigurace

Cíl dokumentu: popsat a zdokumentovat postupy, které vedou k nastavení systému do takového stavu, aby bylo možné systém po instalaci provozovat na základní úrovni.

* Forma dokumentu: textový popis (může být i např. formou okomentovaného config souboru)
* Základní konfigurace sítě (nastavení ip adres, masky, GW, ...)
* Nastavení připojení/komunikace na další systémy (např. DB, web server, SMTP, DNS, NTP, ...), nastavení portů na kterých služba naslouchá, kam data odesílá, …
* Nastavení proxy pro komunikaci, seznam URL (nebo domén), kam systém potřebuje komunikovat (směrem do Internetu), ...
* Spuštění potřebných modulů, agentů, komponent, procesů, registrování knihoven, úprava registrů OS Windows, …
* Nastavení automatických úloh, nastavení systémových účtů, …
* Detailní popis úrovně přístupových oprávnění/aplikačních rolí
* Apod.

#### Záloha, obnova, restart

Cíl dokumentu: popsat a zdokumentovat strategii zálohování systému, jakým způsobem, kdy, kam a jak často jsou zálohována data v rámci daného informačního systému a jakým způsobem se provádí obnova systému po havárii nebo ze zálohy, postupy a konkrétní kroky, které povedou k bezpečnému restartu systému.

* Forma: může být i formou zálohovacího plánu (backup schedule) a disaster recovery plánu, textový popis, návodné obrázky, okomentované příkazy, apod.
* Zálohování
	+ Strategie zálohování systému navržená dodavatelem
	+ Způsob zálohování – plná, přírůstková, rozdílová záloha
	+ Kdy a jak často je záloha prováděna
	+ Jak dlouhou dobu jsou zálohy uloženy a kde
	+ Jak často se provádí testování záloh
* Obnova
	+ Posloupnost kroků (co a jak udělat), které je třeba provést pro obnovu systému nebo jeho části či dat ze zálohy do jeho plně funkčního stavu
	+ Zpracovaný komplexní disaster recovery plán, tedy posloupnost kroků (co a jak udělat), které je třeba provést pro obnovu systému po jeho selhání či nedostupnosti (např. z důvodu kybernetického útoku) do jeho plně funkčního stavu
		- Včetně potřebných zdrojů, jako je např. SW, HW, přístupové údaje, data, parametry disaster recovery prostředí, RTO, apod.
		- Dle tohoto plánu je možné celý systém obnovit v DR prostředí zadavatele
* Restart
	+ Posloupnost kroků, které je třeba provést pro bezpečné restartování systému tak, aby naběhl do původního stavu
		- Např. informování uživatelů, ověření odhlášení všech uživatelů, provedení zálohy systému, restart systému (pořadí konkrétních procesů, služeb, apod.), způsob základní kontroly funkčnosti, výčet služeb, které je potřeba spustit/zkontrolovat, apod.

#### Postupy řešení problémů

Cíl dokumentu: popsat, jakým způsobem se řeší případ nějakého problému, typicky nefunkčnost systému, nefunkčnost části systému, chybové stavy, základní troubleshooting typických use case, apod.

* Základ dokumentace: kontakty (e-mailové adresy, telefonní čísla, url helpdesku)
* V jakém případě, koho a prostřednictvím čeho (e-mailu, helpdesku, sms, telefonu) kontaktovat a jakým způsobem
* Základní troubleshooting často řešených problémů
* Základní chybové stavy (často řešené) – jejich popis a základní způsob odstranění

#### Vazby na jiné systémy, rozhraní, datové vztahy a struktury

Cíl dokumentu: popsat, jakým způsobem je daný systém navázán na jaké systémy, popsat všechna rozhraní a popsat datové vztahy a struktury.

* Forma: textový popis doplněný o schéma
* Výčet systémů, na jaké je daný systém navázán (DB, aplikační servery, fileservery, UI, pracovní stanice/klienti, autentizační brány, zdroje informací /vstupy/, výstupy, datové pumpy, jiné IS, apod.)
* Komunikační protokoly (příp. rozhraní) připojení na jiné systémy
* Porty, ip adresy, identifikátory NIC, API
* Schéma datových toků

#### Monitoring

Cíl dokumentu: popsat a zdokumentovat mechanizmus monitorování a zaznamenávání bezpečnostních a provozních logů a auditních událostí.

* Popis logů informačního aktiva
	+ Výčet a popis všech událostí, které jsou zaznamenávány (př. přihlášení/odhlášení uživatele, provozní/chybové stavy, přidělení/odebrání oprávnění, …)
		- Včetně jejich jednotlivých identifikátorů
		- Včetně popisu jednotlivých polí/atributů události
	+ Způsob uložení zalogovaných událostí
		- Jak jsou události uloženy
		- Kde
			* soubor (včetně cesty k souboru)
			* databáze, včetně:
				+ DB serveru a názvu tabulky, případně tabulek
				+ SQL dotazu pro sestavení view v případě, že událost je uložena do více tabulek
			* vzdálený server (IP adresa, protokol)
		- Jak dlouho jsou uloženy
		- Jak lze konfigurovat
	+ Protokol logování (např. syslog, windows event log, W3C, apod.)
* Popis provozního monitoringu (např. SNMP, síťový monitoring, aplikační monitoring)
	+ Popsat, jakým způsobem je realizován provozní monitoring za účelem identifikace a detekce požadovaných či nestandardních provozních stavů

#### Základní uživatelská příručka

Cíl dokumentu: vytvořit základní návod pro ovládání uživatelského webového rozhraní systému pro běžného uživatele. Zjednodušit běžnému uživateli základní orientaci v uživatelském webovém rozhraní systému.

* Forma dokumentu: textový popis, textový popis doplněný o obrázky
* Popis provedení základních/běžných/rutinních funkcí, kroků a postupů, které uživatel může provádět

#### Základní administrátorská příručka

Cíl dokumentu: vytvořit základní návod pro ovládání administračního rozhraní systému pro administrátora. Zjednodušit privilegovanému uživateli základní orientaci v administračním rozhraní systému.

* Forma dokumentu: textový popis, textový popis doplněný o obrázky
* Popis provedení standardních (základních/běžných/rutinních) operací, které vedou k běžné administraci systému
* Popis provedení nestandardních (málo běžných) operací, pokud je třeba

#### Popis klíčových komponent

Cíl dokumentu: popsat a zdokumentovat účel, význam, úlohu a způsob použití klíčových komponent systému

* Forma dokumentu: textový popis (může být doplněno i o schéma)
* Základní fungování, účel, úloha jednotlivých klíčových komponent + jakou platformou (softwarem) jsou jednotlivé komponenty zajištěny
	+ Např. master (server), agent (klient), různé typy použitých serverů, moduly, zdroje informací, příjemci informací (systémy), apod.