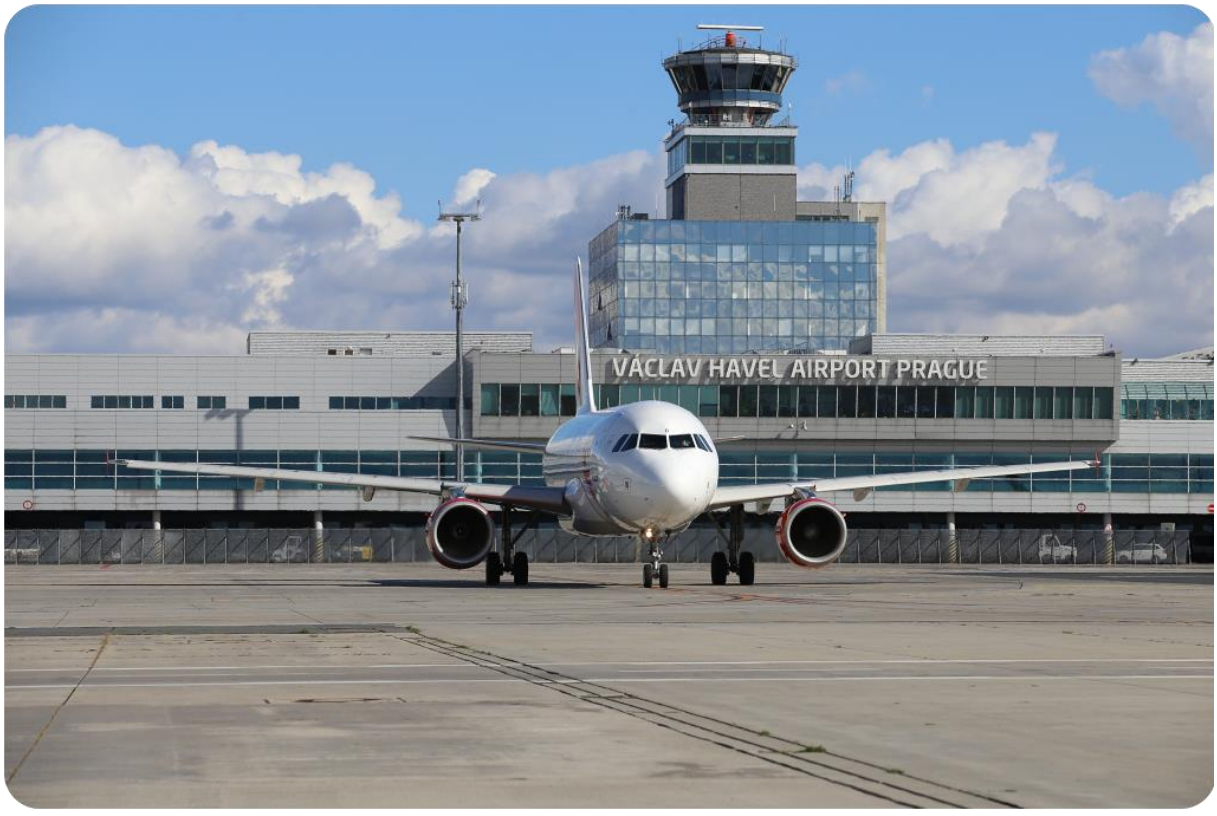
ZÁVAZNÉ TECHNICKÉ STANDARDY PRO ICT PROSTŘEDÍ LETIŠTĚ PRAHA a.s.

(verze 15.10.2020)



Po vytištění nebo vytvoření elektronické kopie je dokument neřízený
Dokument zobrazený na INTRANETU Letiště Praha a.s. je řízen správcem dokumentace LP.

Cíl dokumentu:

Popis technických a technologických standardů pro realizaci výběrových řízení a realizaci projektů v prostředí Letiště Praha a.s.

OBSAH:

I Zkratky a pojmy 3
I.1 Zkratky 3
I.2 Pojmy 3
II Odpovědnosti a pravomoci 4
III Předmět 4
IV Jednotlivé standardy IT prostředí 5
V Standardy pro Cloud a aplikace v něm provozované 17
VI Standardy pro použití mobilních zařízení k přístupu k aplikacím 18
VII Výjimky z uvedených pravidel 19
VIII Související dokumenty 19
IX Přechodná a závěrečná ustanovení 19
X Přílohy 19
X.1 Příloha číslo 1 – Parametry B2B IPSec tunelu 19
XI Změnový list 21

I Zkratky a pojmy

I.1 Zkratky

Zkratka	Vysvětlení
AS	Aplikační server
Azure	Cloud prostředí firmy Microsoft.
DB	Databáze
DMZ	Demilitarizovaná zóna (Samostatná síť oddělená FW. Přístup k počítačům a aplikacím je řízen pravidly FW)
FW	Firewall
IBE	Oddělení informační bezpečnosti
ICT	Informační a komunikační technologie – organizační jednotka LP
OS	Operační systém
M/INF	Manažer týmu Infrastruktura ICT
Ř/IBE	Ředitel OJ IBE
VŘ/ICT	Výkonný ředitel OJ ICT
LKPR	Letiště Praha, a.s.
UNIX, WINDOWS, AIX, Linux, RedHat SUN, SYBASE, IBM, Oracle a další	Zkratky jednotlivých technologií podle výrobce a zaměření
TCP/IP	Síťový komunikační protokol

I.2 Pojmy

Pojem	Vysvětlení
Aplikace	Aplikace/systém zajišťující požadovanou funkcionalitu pro určitou skupinu uživatelů v LP
Interface	Programový prvek pro propojení dvou nebo více rozdílných systémů pro sdílení nebo přenos dat
Login	Unikátní jméno uživatele v prostředí počítačové sítě LP
Uživatel	Pracovník mající přístup do ICT prostředí (identifikován loginem)

II Odpovědnosti a pravomoci

Název Role / Pozice	Popis odpovědností a pravomocí
Administrátor	Osoba provádějící administraci aplikace/systému nebo technologických vrstev (operační systém, databáze, aplikační server,…)
Pracovník	Zaměstnanec LP nebo jeho dceřiných organizací nebo externista (identifikován osobním identifikačním číslem)
Správce aplikace	Osoba na straně ICT, zodpovědná za provoz aplikace, operativní požadavky (odstavení aplikace apod.) a změnové požadavky (změny funkčnosti, úpravy, nastavení aplikace) na aplikaci

III Předmět

Následující standardy jsou závazné pro veškerá zařízení a technologie provozované v interním prostředí počítačové sítě LP bez ohledu na to, kdo je jejím uživatelem.

III.1 Pokud je technologie provozována v režimu částečného hostingu (celá technologie je umístěna v prostorách Letiště Praha a.s., ale je firewallem oddělena od interního prostředí a je pod plnou správou dodavatele), může být po předchozí dohodě udělena výjimka z těchto standardů.

III.2 Standardy se netýkají technologií provozovaných v režimu plného hostování (celá technologie je mimo interní prostředí Letiště Praha a.s.).

III.3 Výjimky uděluje vždy VŘ/ICT na základě dohody s ostatními složkami ICT a IBE.

III.4 Některé technické standardy jsou označeny jako kritické. V těchto případech je vyžadován mimo souhlasu VŘ/ICT i dodatečný výslovný souhlas Ř/IBE. U těchto standardů je uveden znak *

III.5 Za kritické aplikace jsou považovány všechny aplikace, u nichž je požadován chod/podpora 24x7x365, spolehlivost nad 99% nebo doba zotavení pod 30 minut.

III.6 Pokud bude aplikace umístěna v perimetru Internetu, (bude vystavena v Internetu) nebo tvoří součást páteřní infrastruktury, je vždy považována za kritickou.

III.7 U aplikací umístěných v perimetru Internetu, bude vždy požadováno jako součást akceptace předložení pozitivního výsledku penetračních testů dodávané aplikace provedených nezávislým subjektem (schváleným Letiště Praha a.s.). Pokud si to Letiště Praha a.s. vyžádá, může být stejným způsobem požadována i revize zdrojového kódu aplikace.

IV Jednotlivé standardy IT prostředí

IV.1 *Servery*

Následující kapitoly uvádějí přehled technologií pro kritické a ostatní typy systémů.

U kritických aplikací jsou tyto technologie závazné a musí být dodrženy jak typ technologie, tak minimální verze.

U ostatních systémů je možné nasazovat jiné technologie, ale pro jiné systémy, než uvedené v přehledu musí dodavatel zajistit správu vlastními prostředky a zajistit jejich dostupnost dle definovaných podmínek. Přitom je nutné zajistit podporu technologie ze strany výrobce, a to po dobu minimálně **3 let**.

IV.1.1 Sdílená serverová infrastruktura

IV.1.1.1 Aplikace jsou primárně umísťované na prostředky sdílené serverové infrastruktury ve formě virtualizovaných serverů s OS Microsoft Windows Server, Linux na platfomě VMware vSphere

IV.1.1.2 V případech, kdy není možné využít sdílenou serverovou infrastrukturu (vysoké požadavky na výkon, bezpečnostní požadavky, licenční bariéry) je možné se souhlasem VŘ/ICT pro aplikaci vyčlenit samostatný HW

IV.1.1.3 V případě že HW je součástí dodávky aplikace, musí HW splňovat tyto požadavky:

- HW musí být vybavený funkcí vzdálené správy. (Zapnutí/vypnutí, vzdálené ovládání – klávesnice, myš, monitor)
- Důležité HW komponenty musí být redundantní – napájení, chlazení, pevné disky apod.
- HW musí být v rackovém provedení

IV.1.1.4 Sdílená serverová infrastruktura je umístěna ve 2 datových centrech – primárním a záložním. Pro návrh aplikační architektury aplikace pak platí:

IV.1.1.4.1 Kritické aplikace musí být navrženy tak, aby byly odolné vůči výpadku jednotlivých komponent, a i vůči výpadku celého datového centra. Při výpadku primárního datového centra musí aplikace automaticky přejít provoz aplikace do záložního datového centra

IV.1.1.4.2 Ostatní provozní aplikace/systémy jsou umístěny v primárním datovém centru

IV.1.2 Operační systémy

Typ aplikace/systému	Typ OS*	Aktuálně podporované OS
Kritické aplikace	Linux	Linux (RedHat Enterprise 7.5 a vyšší) Linux (distribuce Debian 10 a vyšší)
	Windows	Windows Server 2016 US a vyšší
	AIX	AIX 7.1 a vyšší
Ostatní aplikace/systémy	Linux	Shodné s kategorií kritické vyjma: Linux (distribuce Centos 8 a vyšší)
	Windows	Windows Server 2016 US a vyšší
	AIX	AIX 7.1 a vyšší

IV.1.3 Databázové stroje

Typ aplikace/systému	Typ DB*	Aktuálně podporované verze
Kritické aplikace	ORACLE	19c - Enterprise Edition bez extra licencovaných option packů (Spatial, Partitioning)
	MS SQLServer	MS SQL Server 2017 SP a vyšší
	MySQL	8.0 a vyšší
	MariaDB	10.3. a vyšší

	MongoDB	4.2 a vyšší
	Redis	4.0.4 a vyšší
Ostatní aplikace/systémy	Shodné s kategorií kritické vyjma:	
	PostgreSQL	11.0 a vyšší

IV.1.4 Závazné nastavení DB stroje

IV.1.4.1 MS SQLServer

- Databáze aplikace je prioritně umísťována na sdílený SQL Server určený pro databáze aplikací. Pouze v případě, že aplikace nebude možné umístit na tento sdílený server (z důvodů výkonnostních, bezpečnostních apod.), bude pro aplikaci připraven vlastní SQL Server,
- Pro sdílený MS SQL Server platí následující pravidla:
  - Default Collation sdíleného databázového serveru je „SQL_Latin1_General_CP1_CI_AS“. Collation aplikační databáze je nastavena dle potřeby dané aplikace
  - Aplikace/aplikační účty mají k dispozici oprávnění dbowner k aplikační databázi.
  - Aplikace/aplikační účty nemají k dispozici žádné oprávnění na úrovni administrace SQL Serveru. (Sysadmin, Securityadmin, atd.)
  - Databázové role jsou navázány na skupiny ActiveDirectory
  - Pro aplikačního uživatele je možné využít SQL i Domain autentizaci. Pro autentizaci uživatelů je možné využít pouze Domain autentizaci.

IV.1.4.2 ORACLE

- Databázový server je zařazen v DB perimetru interní sítě a není povolen přímý přístup koncových uživatelů k tomuto serveru.
- Zálohování je prováděno pomocí utility RMAN
- Název databáze může obsahovat pouze znaky A-Z a 0-9.
- Budou dodržovány obdobné bezpečnostní standardy jako u ostatních DB systémů

IV.1.4.3 MySQL / MariaDB

- K databázovému serveru není povolen přímý přístup koncovým uživatelům.

- Název databáze může obsahovat pouze znaky a-z, A-Z a 0-9 a podtržítko (ne na první pozici).

IV.1.4.4 Všechny databáze musí být schopny poskytovat auditní záznamy v požadovaném nastavení, které specifikuje a aktualizuje ICT spolu s IBE v závislosti na dané technologii a vyplývající z povahy důležitosti daného systému. Primárně jsou logovány ACID operace, DDL, přihlašování uživatelů, administrátorské zásahy. Rozsah se může měnit v závislosti na množství generovaných dat a případná změna je vždy aplikována po odsouhlasení ICT a IBE.

IV.2 *Komunikace*

IV.2.1 TCP/IP v4, privátní adresní rozsah pod kontrolou LP, (pokud nebude v požadavcích LP výslovně uvedeno jinak).

IV.2.2 Topologie a síťové prvky jsou pod výhradní správou LP.

IV.2.3 Síťové prostředí se v zásadě rozděluje na 2 kategorie:

IV.2.3.1 DMZ

- Speciální segment lokální sítě vyhrazený pro servery, které jsou zpřístupněné z Internetu.

IV.2.3.2 Interní

- zde jsou servery a zařízení, které nemají povolený přímý přístup do internetu a jsou nedostupná klientům v internetu.

IV.2.3.3 PROXY Letiště
Doplnit reverzní proxy jejich funkčnost a provazby.

IV.2.3.4 Obě tato prostředí jsou chráněna branami firewallu a ve výchozím nastavení nemohou komunikovat ani do internetu ani do ostatních DMZ či interních sítí.

IV.2.4 Zařízení umístěná v DMZ mají zakázáno zahajovat komunikaci se zařízeními v interním prostředí. Pokud je potřeba publikovat na serverech v DMZ prostředí nějaká data, je nutné je tam nahrát z interního prostředí tak, aby přenos zahajovaly

servery v interním prostředí. Požadavky na výjimku z tohoto pravidla jsou podmíněny předchozím souhlasem M/SDS a Ř/IBE, popř. VŘ/ICT.

IV.2.4.1 Pokud jsou v DMZ umístěny servery ve vícevrstvé architektuře, tak všechny podřízené servery (aplikační či databázové) musí být rovněž v DMZ prostředí. Tento bod respektuje požadavek ohledně zakázaného navazování komunikace z DMZ do interního prostředí.

IV.2.5 Uživatelé smí připojovat do datové sítě pouze schválená koncová zařízení a to jen v místech, která jim k tomu byla určena. Je výslovně zakázáno připojovat zařízení typu směrovačů, přepínačů či bezdrátových bodů. Požadavky na výjimku z tohoto pravidla jsou podmíněny předchozím souhlasem M/SDS a Ř/IBE, popř. VŘ/ICT.

IV.2.6 Vlastní oblast tvoří cloudové prostředí, které je ze síťového pohledu pokládáno za externí a služby cloudu jsou pouze integrovány s on-premise. Cloud je v této architektuře pokládán za méně důvěryhodný apriori a jsou na něj aplikovány obdobné principy jako u DMZ.

IV.2.7 Na koncová zařízení bude uplatněný hardening.

IV.3 *Vzdálený přístup*

IV.3.1 *Uživatelský vzdálený přístup*

IV.3.1.1 Pro vzdálený přístup do prostředí Letiště Praha určuje pravidla pracovní postup Pravidla VPN přístupu.

IV.3.2 B2B vzdálený přístup

IV.3.2.1 B2B vzdálený přístup je určen pro trvalé propojení interního prostředí Letiště Praha a prostředí externí společnosti pomocí IPSec tunelu. Tento přístup je určen pouze pro aplikační účely. Tento B2B vzdálený přístup nelze požadovat pro účely vzdálené správy, pro tyto účely je určen Uživatelský vzdálený přístup.

IV.3.2.2 Externí firmy s tímto přístupem musí garantovat, že k systémům v jejich prostředí, využívajících tohoto propojení, nemají přístup jiné subjekty, tzn. nejedná se o sdílenou službu.

IV.3.2.3 Popis parametrů IPSec tunelu je uveden v Příloze č. 1

IV.3.2.4 Realizace B2B vzdáleného přístupu jsou podmíněny předchozím souhlasem M/SDS, popř. VŘ/ICT.

IV.4 *Aplikační servery*

Aktuálně provozované:

Typ AS	Aktuálně provozované AS
Apache Tomcat	Tomcat 8.x a vyšší
JBoss	JBoss 7.2.0 a vyšší
IIS	IIS 10 a vyšší

IV.4.1 Aplikační Windows Servery jsou pravidelně 1x měsíčně patchovány za použití služby WSUS. Poznámka: S touto skutečností je potřeba počítat při návrhu aplikační architektury aplikace, tak aby bylo dosaženo požadované SLA aplikace.

IV.4.2 Na všech aplikačních Windows Serverech je provozován antivirový systém Forefront nebo Windows Defender.

IV.4.3 Všechny Windows servery jsou pravidelně automaticky skenovány pomocí nástroje pro skenování zranitelností oddělení IBE. Četnost skenování je určena dle kritičnosti systému a dle četnosti provádění aktualizací.

IV.4.4 Na Windows Serverech je instalován SCOM agent pro zajištění monitoringu serveru.

IV.4.5 Na Windows Serverech je nainstalován agent BitDeffender sledující v reálném čase chování serveru a případně zasahující do jeho běhu při identifikaci bezpečnostního incidentu. O tomto incidentu je vždy veden záznam jak na lokální úrovni, tak v centrální správě a SIEM.

IV.4.6 Na Windows Serverech jsou sbírány logy pomocí WEF kolektoru v případě, že server je členem domény. Pokud není v doméně, pak na server bude nainstalovaný standalone agent SIEM dle specifikace oddělení IBE.

IV.5 *WWW aplikace*

IV.5.1 Strana LP:

	WWW server *	Podporované verze
Všechny aplikace	Apache MS IIS nginx	2.4 a vyšší IIS 10 a vyšší Nginx 1.18.0 a vyšší

Konkrétní verzi sdělí na vyžádání M/INF. Je povoleno použití PHP v. 7.4 a vyšší (v interním prostředí - konkrétní verze podporovaného SW se odvozuje z aktuálních verzí v oficiálních repozitářích použitého OS).

Pro použití JAVA appletů a ActiveX komponent je nutno získat předchozí souhlas M/INF.

IV.5.2 Strana klienta

- Podpora prohlížeče Chrome – aktuální verze, zpětně kompatibilní od verze 86
- Podpora prohlížeče Edge Chromium – aktuální verze, zpětně kompatibilní od verze
- Podpora prohlížeče Firefox – aktuální verze, zpětně kompatibilní od verze 75

IV.6 *E-mail, messaging*

IV.6.1 Interní poštovní systém je založený na službě Microsoft Exchange Online.

IV.6.2 Pro aplikační přístup k emailové schránce je defaultně využíván služba EWS – Exchange Web Services. Použití dalších protokolů - IMAP, POP3 pouze se souhlasem VŘ/ICT

IV.6.3 Pro odesílání emailu v rámci aplikace v interním prostředí je možné pouze při využití TLS a autentizace loginem a heslem aplikačního doménového uživatele. Komunikace z interních aplikačních serverů je směrována na interní SMTP server. Použití Open Relay není podporováno.

IV.6.4 Není povoleno automatizované odesílání emailů jménem uživatelů. (atribut „FROM“ emailové zprávy obsahuje adresu aplikačního uživatele).

IV.6.5 Aplikace, která odesílá větší množství emailů najednou (hromadný mailing), musí umožňovat odesílání emailů po částech, popř. rozložit odeslání v čase.

IV.7 *Autentizace*

IV.7.1 Veškerá pravidla týkající se autentizace jsou uvedena ve směrnici Správa identit a přístupů.

IV.7.2 Základní repository pro správu uživatelů je Active Directory. Pro přístup k LDAP je třeba využít zabezpečené připojení pomocí protokolu LDAPS.

IV.7.3 On-premises prostředí je synchronizováno s cloudovým prostředím Azure Active Directory a to pro autentizace v Azure.

IV.7.4 Pro autentizaci uživatelů v interním prostředí v rámci Active Directory je využíván protokol Kerberos. Při využití Kerberos delegace musí být delegace omezena přímo na konkrétní službu. Případné jiné autentizace podléhají schvalování ICT LP a IBE LP.

IV.7.5 Pro autentizaci on-premises uživatelů přistupujících z prostředí cloudu resp. Internetu je možné využít služby ADFS

IV.7.6 Pro přihlašování k databázím a aplikačním serverům je preferována integrovaná Windows autentizace.

IV.7.7 V případě, že není použita integrovaná autentizace, tak je vyžadováno využití šifrovaného spojení.

IV.7.8 Uživatelské přihlašovací údaje nesmí být uložené ve volně čitelné podobě, ale musí být chráněny v šifrovaném úložišti s omezených přístupem pouze pro autorizované osoby a služby/aplikace.

IV.7.9 Pro správu klíčů a jejich zabezpečení v prostředí Microsoft Azure je vyžadováno užití služby Azure Key Vault.

IV.7.10 Uživatelské účty jak jmenné, tak systémové a technické musí odpovídat jmenné konvenci a evidenci v interní aplikaci “Evidence loginů”.

IV.7.11 Pro cloudové prostředí je vyžadována MFA autentizace pro privilegované účty.

IV.7.12 Pro autentizaci systémových a technických účtu nesmí být kombinovány produkční účty s testovacími v jednom prostředí. Testovací a produkční účty musí být rozlišeny jmennou konvencí.

IV.7.13 Veškerá autentizace musí být vždy auditována a auditní záznamy musí být předávány do SIEM.

IV.8 *Prostředí Windows Serverové Infrastruktury*

IV.8.1 *Active Directory*

IV.8.1.1 Domain functional Level domény CAH je nastaven na „Windows server 2016“

IV.8.1.2 Pro autentizaci uživatelů v ActiveDirectory je primárně používán protokol Kerberos. Použití LM a NTLM je zakázáno. Se souhlasem VŘ/ICT a Ř/IBE je možné využít NTLMv2. Při použití Basic autentizace je nutné využít šifrované spojení viz kapitola “Autentizace”.

IV.8.1.3 Aplikace nesmí v rutinním provozu vyžadovat v Active Directory žádná oprávnění nad rámec běžného uživatelského účtu

IV.8.2 *Aplikační Windows Servery*

IV.8.2.1 Aplikace nesmí pro svůj běh vyžadovat interaktivní přihlášení k serveru. To znamená, že musí fungovat v režimu „služba“, „naplánovaná úloha“ apod.

IV.8.2.2 Aplikační účet (lokální serverový resp. doménový) nesmí být využíván k interaktivnímu přihlašování k serveru.

IV.8.2.3 Bez schválení OJ WIN je zakázáno měnit systémové parametry serveru – tj. parametry na úrovni operačního systému. Např. síťová nastavení, nastavení časového pásma, nastavení lokálních uživatelů a skupin atd.

IV.8.2.4 Instalace programových souborů aplikace musí být umístěna do standardních adresářů „C:\Program Files” resp “C:\Program Files (x86)”

IV.8.2.5 Data aplikace, popř. log soubory aplikace překračující celkovou velikost 5GB musí být směrované mimo systémový disk C:

IV.8.2.6 Pokud existuje propojení aplikace – databáze, aplikace nesmí vyžadovat instalaci na stejném serveru jako databáze.

IV.8.2.7 Aplikační server má nastavené bezpečnostní politiky odpovídající doporučení NIST případně IBE dle specifik LP.

IV.8.3 Výjimky z těchto pravidel podléhají schválení ICT LP. Výjimky týkající se informační bezpečnosti schvaluje IBE LP.

IV.9 *Koncové stanice*

IV.9.1 **Běžné uživatelské koncové stanice**

IV.9.1.1 OS: Windows 10 Enterprise 64-bit

IV.9.1.2 Kancelářský balík: MS Office Standard/Professional-2016 CZ/US, O365 CZ/US *

IV.9.1.3 Uživatelé mají pouze práva „User“

IV.9.1.4 Počítače jsou pravidelně patchovány službou WSUS

IV.9.1.5 Na počítačích je provozován antivirový systém Windows Defender a BitDeffender.

IV.9.1.6 Koncové stanice mají nastavené bezpečnostní politiky odpovídající doporučení NIST, případně IBE dle specifik LP.

IV.9.2 **Omezení pro aplikace/klienty**

IV.9.2.1 Aplikace pro svůj běh nesmí využívat „vyšší“ oprávnění než „User“

IV.9.2.2 Aplikace musí být kompatibilní s bezpečnostní technologií UAC

IV.9.2.3 Aplikace musí podporovat tzv. „tichou instalaci“

IV.9.2.4 Aplikace musí fungovat pod virtualizační platformou Microsoft Application Virtualization App-V

IV.10 *Terminálový přístup*

IV.10.1 Jsou podporovány platformy Microsoft Remote Desktop Services (RDS).

IV.10.2 Běžně není podporován RDP kanál pro periferie (tiskárny, COM porty atd.). Případné využití vzdáleného přístupu k těmto službám podléhá schválení ICT a IBE.

IV.11 *Virtualizace*

IV.11.1 Pro virtualizaci serverů se používá platforma VMWare. Aktuální verze VMWare vSphere 6.5.

IV.11.2 Při návrhu aplikační architektury je možné využít technologií VMware HA pro zajištění vysoké dostupnosti virtuálního serveru.

IV.11.3 Pro virtualizaci aplikací na koncových stanicích je používána platforma APP-V verze 5.

IV.12 *Vývojové prostředí*

IV.12.1 Doporučené vývojové platformy jsou následující:

IV.12.1.1 Desktopová vývojová prostředí a IDE

- Visual Studio 2019 a vyšší
- Visual Studio Code
- SQL Server Management Studio 18 a vyšší
- PowerShell ISE 5.0 a vyššší
- Apache NetBeans 12

IV.12.1.2 Nástroje pro analytické práce a modelování

- Enterprise Architect 14 a vyšší
- Archimate 3.0 a vyšší
- Visio 2016
- Visual Studio 2019 a vyšší

IV.12.2 Správa zdrojových kódů - Source Code Management SCM

On-Premise:

- Subversion 1.13 a vyšší
- Git 2.25 a vyšší

Cloud based:

- GitHub
- Azure Repos - DevOps (VSTS)

IV.12.3 Koncové stanice (PC)

- Visual Studio C++ Redistributable Runtime 2017, 2019
- OpenJDK 1.7 a vyšší
- .NET 4.7.1 Framework a vyšší
- .NET Core 3.1 a vyšší
- Powershell 5.1 a vyšší (https://docs.microsoft.com/en-us/powershell/)

IV.12.4 Podporované runtime prostředí na serverech

- JAVA RE 8, v případě nutnosti JAVA SE 15 a vyšší
- OpenJDK 1.7 a vyšší
- .NET Framework 4.7.1 a vyšší
- .NET Core 3.1 a vyšší
- Powershell 5.1 a vyšší
- Powershell Core (https://docs.microsoft.com/en-us/powershell/)
- PHP 7.4 a vyšší
- PERL, Shell, atd. - pouze po předchozím schválení VŘ/ICT.

IV.13 *Nasazování aplikací (deployment)*

Nasazování aplikací musí probíhat v několika fázích a být dodrženy technologické a bezpečnostní standardy.
Základní principy:

- V prostředí Microsoft Azure DevOps (dále jen Azure DevOps) pro aplikaci/systém je založen projekt do něhož mají přístup uživatelé s funkčními rolemi:
    - Projektový manažer
    - Vývojář
    - Aplikační správce
    - Infrastrukturní správce
    - Specialista informační bezpečnosti
    - Tester/uživatel

  Konkrétnímu uživateli může být přidělena více než 1 funkční role.
- Zdrojový kód systému/aplikace je vždy uložen v repository Letiště Praha (viz.kapitola IV.12.2)
- Cílem je nasazovat aplikace maximálně automatizovaně.
- V prostředí Azure DevOps budou nastaveny pipelines pro nasazení, kontrolu kódu včetně bezpečnostní analýzy a odsouhlasení zodpovědnou osobou na jednotlivá prostředí.
- Nasazení nové verze na vývojové prostředí není nezbytný souhlas role tester/uživatel. V ostatních případech toto potvrzení je součástí definice pipeline.
- Veškeré úpravy kódu musí být vždy v prostředí DevOps doplněny o dokumentaci/popis změn.
- Aplikace jsou **vždy** nasazovány v pořadí: vývojové prostředí, testovací prostředí, stage a produkční prostředí (minimem jsou prostředí testovací a produkční)
- Vývojové prostředí – prostředí pro vývoj aplikace. Je zde přípustná instalace debugovacích nástrojů schválených IBE
- Testovací prostředí umožňuje konfigurace, které nejsou nastavovány s ohledem na bezpečnost, výkon a další parametry, ale primárně na ladění funkčnosti aplikace
- Stage (/akceptační) prostředí odráží produkční prostředí a je s ním prakticky identické, co do technické konfigurace, ale liší se v datech, která nejsou produkční a nebo nejsou aktuální. V tomto prostředí je možné mít nainstalované některé z nástrojů pro ladění aplikace, ale bez dopadu na shodu konfigurace stage prostředí s produkcí. Cílem je otestování aplikace v prostředí s ohledem na kompatibilitu s produkčním prostředím a minimalizaci rizika nasazení aplikace do produkce.
- Produkční prostředí již obsahuje ostrá data a zde musí být zachovány maximální bezpečnostní, výkonností a další produkční parametry.

IV.14 *Jednotlivé standardy IT prostředí pro aplikace v DMZ zóně*

Pro aplikace provozované v DMZ platí následující standardy:

IV.14.1 HW PLATFORMA: Intel 64bit

IV.14.2 OS: RedHat Enterprise Linux - x86_64 (release 7.x a vyšší), Debian 10 a vyššíOS: Windows Server 2016 US 64 a vyšší

IV.14.3 DB:
- MySQL 5.7 a vyšší (pouze pro tzv. necitlivá data)
- MariaDB 10.1 a vyšší (pouze pro tzv. necitlivá data)

IV.14.4 Aplikační server
- Apache 2.2 a vyšší
- nginx
- Tomcat /JBoss
- IIS 10 a vyšší

IV.14.5 Skriptovací jazyky
- PHP 7.4 a vyšší
- PERL 5.28 a vyšší
- Bash
- Powershell Core 6.0 a vyšší

Konkrétní verzi sdělí na vyžádání M/INF.

V Standardy pro Cloud a aplikace v něm provozované

V.1 Cloudové prostředí je z pohledu Letiště externí a méně důvěryhodné prostředí ve srovnání s interní on-premise sítí Letiště.

V.2 Cloudové prostředí je integrováno s centrální správou uživatelů ve Windows Active Directory propojené s Azure AD pomocí technologie Azure AD Connect.

V.3 Aplikace a systémy běžící v cloud prostředí a využívající jakýkoliv z prostředků Letiště mohou pro autentizaci využívat pouze Azure AD. Není povolen přímý ani nepřímý přístup z cloud prostředí při autentizaci na on-premise služby Active Directory.

V.4 Aplikace mohou případně využívat vlastní aplikační autentizaci se schválením IBE a pokud jsou splněný minimální podmínky se zabezpečením autentizačních údajů.

V.5 Pokud jakákoliv aplikace nebo systém v cloud prostředí chtějí využívat on-premise služby Letiště, musí k tomu použít architekturu Azure ServiceBus Relay.

V.6 Pokud aplikace nedokáže Azure ServiceBus Relay využít, může využít aplikační rozhraní publikované v DMZ a které tyto služby zprostředkovává pomocí zveřejněného API.

V.7 API je poskytováno ve formě webové služby nebo REST API. Případně je možné domluvit další formáty pro výměnu dat, které podléhají schválení příslušného oddělení ICT a IBE.

V.8 Veškerá komunikace s tímto API musí probíhat šifrovaně a na základě autentizace volajícího klienta.

V.9 Aplikace přistupující k API Letiště libovolným způsobem musí autentizační hesla nebo tokeny vždy ukládat v šifrované podobě v chráněném “vault” prostředí, kde pouze oprávněné osoby mají přístup. Hesla ani tokeny nesmí být nikdy uložena ve volně přístupné a čitelné podobě viz kapitola “Autentizace”.

V.10 Požadavky na výjimku z tohoto pravidla jsou podmíněny předchozím souhlasem Ř/INF, popř. VŘ/ICT.

V.11 Provoz aplikací v jednotlivých prostředí musí být optimalizován s ohledem na jejich charakter s cílem minimalizovat náklady. To znamená dostupnost testovacích, vývojových a dalších prostředí pouze v časech kdy mohou být užívány. V opačném případě prostředí by měla být vypnuta. Tento proces by měl být automatizován nebo vyžadující pouze minimální zásah administrátora.

VI Standardy pro použití mobilních zařízení k přístupu k aplikacím

Tyto standardy se budou řídit obdobnými bezpečnostními a technologickými principy LP jako v případě ostatních zařízení.

Tyto přístupy lze rozdělit dle prostředí, ze kterého přistupují na interní a externí.

VI.1 *Přístup z interního prostředí*

Pokud se jedná o zařízení připojená v interní síti, tedy zařízení s OS MS Windows a zařazená do CAH Active Directory, pak lze přistupovat k libovolným interním aplikacím.

VI.2 *Přístup z důvěryhodného externího prostředí*

Důvěryhodné externí prostředí je privátní zabezpečený přístup např. 3G/4G přístup s privátním APN operátora či bezdrátová síť v areálu letiště zabezpečená autentizací a šifrováním přenosového kanálu.

Přístupy k interním aplikacím z tohoto prostředí podléhají explicitnímu schvalování Ř/INF, popř. VŘ/ICT po zvážení rizik z tohoto plynoucích.

VI.3 *Přístup z nedůvěryhodného externího prostředí*

Jedná se jak o přístup z internetu – např. 3G/4G připojení, tak i přístup přes veřejnou bezdrátovou síť v areálu letiště. Zařízení připojená v tomto prostředí mohou přistupovat pouze k aplikacím, které jsou umístěny v DMZ nebo v cloudu a jsou dostupná z internetu.

VII Výjimky z uvedených pravidel

Všechny výjimky z výše uvedených standardů jsou možné aplikovat pouze po výslovném schválení VŘ/ICT.

Výjimky týkající se informační bezpečnosti pak podléhají schválení Ř/IBE.

VIII Související dokumenty

(1) Směrnice „Správa identit a přístupů“
(2) Směrnice „Pravidla antivirové ochrany“
(3) Směrnice „Pravidla VPN přístupu“
(4) Směrnice „Správa firewallů a síťových prvků“
(5) Směrnice „Správa šifrovacích klíčů a kryptografická podpora systémů“

IX Přechodná a závěrečná ustanovení

(1) Režim kontroly aktuálnosti znění směrnice je dva roky od vydání poslední platné verze.
(2) V případě zásadních změn bude směrnice přepracována operativně dle potřeby.

X Přílohy

X.1 Příloha číslo 1 – Parametry B2B IPSec tunelu

Partner info		
Company:		***LP***
Address:		

City:		Prague
Country:		CZE
VPN endpoint		
Supplier:		Juniper
Type:		SRX 1400
Public IP Peer address:		
Mode	Main	
IKE Parameters - Phase 1		
Authentication Mode:	preshared key	
Preshared Key:	via sms	
Authentication Algorithm:	SHA2-256	
Encryption Algorithm:	AES-256-CBC	
Diffie-Hellman Group:	14	
Aggressive mode:	disabled	
Lifetime Measure:	time	
Lifetime (seconds):	28800	
IPSEC Parameters - Phase 2		
Protocol:	ESP	
Authentication Algorithm:	SHA2-256	
Encryption Algorithm:	AES-256-CBC	
Encapsulation Mode:	tunnel	
PFS:	no	
PFS Group:	no	
Lifetime Measure:	time	
Lifetime (seconds):	3600	
Local network		
Test IP for ICMP (ping)		
Technical Contact		
	email: phone:	email: phone:

	comment:	comment:

XI Změnový list

Datum	Důvod / charakter změny	Podpis

Konec textu vnitřní normy
"ZÁVAZNÉ TECHNICKÉ STANDARDY PRO ICT PROSTŘEDÍ"
Následuje příloha/y