Příloha č. 7 - Bezpečnostní požadavky MD na aplikace

Pokyny pro vyplnění	
Zápis je dovolen pouze do sloupců "Míra naplnění požadavku" a "Komentář".	
Sloupec "Míra naplnění požadavku" • pole musí být vyplněno; • hodnota je vybírána z níže	Sloupec "Komentář" • pole musí být vyplněno; • musí obsahovat stručný popis způsobu naplnění/nenaplnění požadavku a/nebo další relevantní informace; • nevyplnění pole je chápáno stejně jako vyplnění pole "Míra naplnění požadavku" hodnotou "Nesplňuje".
Plně splňuje	
Částečně splňuje	
Nesplňuje	
N/A	

	Bezpečnostní požadavky		Vyjádření dodavatele	
			Míra naplnění požadavku	Komentář
1	**Obecné bezpečnostní požadavky**			
1.1	Obecné bezpečnostní požadavky	Dodavatel předloží podrobný bezpečnostní koncept řešení, který bude podléhat schválení. Veškeré dodané bezpečnostní dokumenty jsou chápány jako součást technických specifikací nabízených řešení a služeb a tudíž závaznou součástí smlouvy.	Plně splňuje	bude dodáno
1.2	Obecné bezpečnostní požadavky	Síťové interfacy pro služby, správu a podporu dodaných zařízení musí podporovat segmentaci sítě dle dokumentace MD.	Plně splňuje	standardní funkčnost - možno provozovat vprostřed více síťových segmentů
1.3	Obecné bezpečnostní požadavky	Dodané řešení musí podporovat nezbytné mechanismy pro přesnou synchronizaci času (protokol NTP) pro společné součásti architektury i jednotlivé služby (servery i aplikace).	Plně splňuje	Využívá služeb domény Active Directory
2	**Identifikace a autentizace**			
2.1	Identifikace a autentizace	Před přiřazením uživatelského jména nebo jiných identifikačních mechanismů přístupu k prostředkům IS musí uživatelé projít registrační procedurou, která potvrdí jejich totožnost způsobem, který je nezaměnitelný a personalizovaný.	Plně splňuje	Využívá služeb domény Active Directory
2.2	Identifikace a autentizace	Každý uživatel musí mít vlastní uživatelské jméno; sdílení přístupových údajů více uživateli není dovoleno. Stejně tak každé uživatelské jméno musí mít právě jednoho vlastníka zodpovědného za jeho použití.	Plně splňuje	Využívá služeb domény Active Directory
2.3	Identifikace a autentizace	Obrazovka pro zadání přístupových údajů (resp. jakékoliv zobrazení před ověřením identity uživatele) musí poskytnout jen nezbytné minimum informací (neposkytují informace z operačního systému, informace o organizaci, neveřejné informace apod.). Hesla nesmí být při zadávání (ani v jiných případech) viditelná (např. se nahradí definovaným znakem).	Plně splňuje	standardní funkčnost - zobrazovány pouze nezbytné informace
2.4	Identifikace a autentizace	Uživatelský účet musí být automaticky zablokován při 9 a více po sobě následujících neúspěšných pokusech o přihlášení minimálně na 30 minut nebo do zásahu administrátora.	Plně splňuje	Využívá služeb domény Active Directory
2.5	Identifikace a autentizace	Musí být definované procedury pro generování, distribuci a změny hesel.	Plně splňuje	Využívá služeb domény Active Directory
2.6	Identifikace a autentizace	Iniciační heslo uživatele nebo heslo předávané při jeho resetu (např. z důvodu zapomenutí uživatelem) musí být vždy různé a náhodné (a nesmí odpovídat uživatelskému jménu, ani z něj být odvozeno); při nastavování nebo resetování hesla nesmí být použito stejné. Uživatel musí být donucen systémem si iniciační (nebo resetované) heslo při prvním použití změnit.	Plně splňuje	Využívá služeb domény Active Directory
2.7	Identifikace a autentizace	Aby byla garantována důvěrnost a integrita hesel, musí být předávána jiným komunikačním kanálem, než k nim příslušná uživatelská jména. Hesla nesmí být předávána v otevřeném textu přes veřejné/externí sítě.	Plně splňuje	standardní funkčnost
2.8	Identifikace a autentizace	Změna hesla musí být vynucena, pokud nebylo změněno v posledních 3-18 měsících (administrátorem konfigurovatelný parametr). Uživateli musí být umožněna změna hesla kdykoliv; opakovaná změna hesla ale nejdříve po 30 minutách. Mechanismus pro změnu hesla (bez ohledu na to zda uživatel mění heslo o své vůli, nebo je změna vynucena) musí splňovat následující: • hesla nesmí být při vkládání zobrazena v čitelné podobě; • před změnou hesla musí být vyžadováno zadání stávajícího hesla; • nové heslo musí být požadováno zadat dvakrát (jako prevence překlepů); • opakování libovolného z posledních 12 použitých hesle nesmí být dovoleno; • délka a další požadované parametry hesla musí být ověřeny před zapsáním změny (pokud nové heslo nevyhovuje, musí být uživatel upozorněn a vyzván z úpravě nového hesla) Hesla nastavená při instalaci aplikace/programu/systému musí být změněna. Je doporučeno změnit i názvy defaultních/obecných účtů.	Plně splňuje	Využívá služeb domény Active Directory
2.9	Identifikace a autentizace	Nastavená politika pro hesla musí splňovat minimálně požadavky Vyhlášky o kybernetické bezpečnosti č. 82/2018	Plně splňuje	Využívá služeb domény Active Directory
2.10	Identifikace a autentizace	Aby byla garantována důvěrnost a integrita hesel, nesmí být ukládána v čitelném textu, ale šifrována nebo musí být použito jednosměrné hash funkce. Přístup k uloženým heslům musí být řízen.	Plně splňuje	standardní funkčnost - ukládná hesla jsou šifrována
2.11	Identifikace a autentizace	Při použití uživatelských certifikátů musí být definovány procedury pro registraci, generování, obnovu, revokaci a likvidaci těchto certifikátů. Preferovány jsou certifikáty JIP/KAAS.	Plně splňuje	ve shodě s bezp. politikou
2.12	Identifikace a autentizace	Systém, který pro identifikaci, autentizaci a autorizaci uživatele používá digitální certifikáty, musí ověřit pravost a platnost certifikátů a ověřit, že certifikát nebyl revokován, před umožněním přístupu uživateli. Ověřením certifikátu je myšlena kontrola proti seznamu zrušených certifikátů (CRL – Certification Revocation List), pomocí protokolu OCSP (Online Certificate Status Protocol), nebo jiných mechanismů, které zaručují, že certifikát je platný a nebyl zrušen.	n/a	digitální certifikáty nejsou pro identifikaci a autentizaci využívány
2.13	Identifikace a autentizace	Řešení dodavatele musí vyžadovat autentizaci jak pro operační systém, tak pro aplikace, které jsou nezbytné pro jeho fungování. Ověření musí být vyžadováno jak pro přístup z fyzické konzole, tak pro vzdálený přístup k systému či aplikacím, které přístup ze sítě umožňují.	Plně splňuje	standardní funkčnost - bez ověření nelze spustit žádnou aplikaci

2.14	Identifikace a autentizace	Řešení dodavatele musí být schopno integrace do systému centralizovaného ověřování (například systémy založené na protokolech LDAP, RADIUS nebo TACACS +) v operačním systému i v aplikacích, které jsou nezbytné pro jeho fungování, při ověřování, autorizaci a logování činnosti uživatelů a při správě hesel s cílem jednoznačně identifikovat totožnost osoby, která provádí přístup. Preferována je integrace s AD prostředím MD.	Plně splňuje	Využívá služeb domény Active Directory
2.15	Identifikace a autentizace	Síťový přístup k řešení dodavatele nesmí zobrazovat informace (banner) vztahující se k serveru, jako je operační systém, aplikace, verze použitého SW apod.	Plně splňuje	standardní funkčnost - není zobrazováno
3	**Řízení přístupu**			
3.1	Řízení přístupu	Každý uživatel systému musí být jednoznačně identifikován svým uživatelským jménem. Uživatelem se rozumí osoby nebo procesy (služby), které k systému přistupují.	Plně splňuje	identifikace uživatelů standardní součástí
3.2	Řízení přístupu	Je preferováno řízení přístupu založené na uživatelských rolích proti diskrétnímu přidělování a kontrole oprávnění uživatelských jednotlivým účtům. Informační systém musí řídit přístup nejen uživatelů, ale i všech dalších systému a aplikací, které k němu přistupují. Systém musí logovat jak přístupy autorizovaných uživatelů, tak neautorizované (anonymní) přístupy i pokusy o neoprávněný přístup.	Plně splňuje	přístup řízen na základě rolí s jemným nastavením přístupových práv
3.3	Řízení přístupu	Hesla musí být chráněna před zneužitím neoprávněným uživatelem. Při vytváření nového účtu je uživateli dočasně přiděleno heslo, které je povinen neprodleně změnit.	Plně splňuje	Využívá služeb domény Active Directory
3.4	Řízení přístupu	V případě použití certifikátů pro přístup k systému jsou povoleny certifikáty vydané Certifikačními Autoritami schválenými MD, preferovaný je systém JIP/KAAS.	n/a	digitální certifikáty nejsou pro identifikaci a autentizaci využívány
3.5	Řízení přístupu	Na produkčním prostředí nesmí být zřízen účet vývojáře aplikací. Takový účet smí být zřízen pouze na vývojovém/testovacím prostředí a může mít nastaveny parametry obdobné účtu administrátora aplikace.	Plně splňuje	vývojářský účet není pro produkční prostředí potřeba
3.6	Řízení přístupu	Uživatelské jméno a heslo předávané po síti musí být vždy šifrované. Stejně tak musí být šifrované staré i nové heslo při procesu jeho změny uživatelem (dobrovolném i vynuceném). Pro autentizaci je možné použití externích systému jako Kerberos či adresářových služeb jako LDAP nebo AD apod.	Plně splňuje	tlusté aplikace využívají šifrovanou komunikaci, webové aplikace využívají protkol https. Pro správu účtů a hesel zpravidla využíváno služeb domény Active Directory.
3.7	Řízení přístupu	Vzdálených přístup administrátorů provádějících správu systému včetně nastavování uživatelských hesel a správy účtů musí být šifrován.	Plně splňuje	závisí na komunikačních knálech použitých pro vzdálený přístup
3.8	Řízení přístupu	Informační systém nesmí uživateli zobrazovat funkce a volby, ke kterým uživatel není autorizován (nemá přístup).	Plně splňuje	standardní funkčnost
3.9	Řízení přístupu	Po 15 minutách (parametr musí být konfigurovatelný administrátorem) neaktivity musí systém uživatele automaticky odhlásit a zobrazit příslušnou informační obrazovku.	Plně splňuje	Využívá služeb domény Active Directory
3.10	Řízení přístupu	Autentizace (a/nebo autorizace) založená výhradně na zdrojové adrese (IP, MAC apod.) uživatelského zařízení není dovolena. Ověření zdrojové adresy je možné použít jako doplnění k autentizaci, v takovém případě ale musí být tato možnost nastavitelná administrátorem.	Plně splňuje	Řízení přístupu na základě IP/MAC adresy není používáno
3.11	Řízení přístupu	Vzdálený přístup dodavatele k údržbě nebo diagnostice interního systému musí být předem schválen vlastníkem systému a bude přísně omezen na dobu potřebnou k provedení požadované služby.	Plně splňuje	standardní funkčnost
3.12	Řízení přístupu	Síťový i fyzický přístup ke konfiguračním portům a diagnostice síťových zařízení a systémů musí být řízen.	Plně splňuje	závisí na implementaci vytvořené zákazníkem
3.13	Řízení přístupu	Spouštění a běh služeb a/nebo aplikací pod administrátorským oprávněním (root, administrátor a další systémové účty) je zakázáno.	Plně splňuje	administrrátorská oprávnění nejsou pro běh systému potřebná
3.14	Řízení přístupu	Je zakázáno přihlašovat se přímo k výchozím systémovým účtům určeným pro správu. Pro každou fyzickou osobu, která provádí správu, musí být vytvořen osobní účet, ze kterého se pak k systémovému účtu přihlásí pomocí nástroje "runas" nebo "su" či podobného.	Plně splňuje	standardní funkčnost
3.15	Řízení přístupu	Zřizování skupinových účtů a sdílení uživatelských účtů není dovoleno. Je-li zřízení skupinového účtu nezbytné, je zakázáno s k takovému účtu přihlašovat přímo; uživatel se přihlásí ke svému účtu a následně použije k přihlášení ke skupinovému účtu nástroj "runas" nebo "su" či podobný.	Plně splňuje	skupinové účty nejsou používány. Je možno využít mechanismu záastupu - akce provedené zastupujícím jsou logovány
3.16	Řízení přístupu	Řešení musí umožňovat implementaci přístupových profilů tak, aby byla pro každého uživatele použita příslušná úroveň oprávnění.	Plně splňuje	přístup řízen na základě rolí s jemným nastavením přístupových práv
3.17	Řízení přístupu	Řešení musí obsahovat minimálně dvě různé správcovské role – supervizor, který může nastavovat parametry v rámci aplikačního prostředí a administrátor, který je oprávněn provádět změny konfigurace systému, upgrady SW apod.	Plně splňuje	Systém umožňuje velmi detailní přidělování přístupových oprávnění, je tedy možno vytvořit dle potřeby více správcovských rolí
3.18	Řízení přístupu	Řešení musí podporovat konfiguraci fyzických přístupových portů a zakázat ty, které se nepoužívají. Nevyužité fyzické porty v produkčním systému musí být explicitně zakázány.	Plně splňuje	řešeno na úrovni operačního systému hostitelského serveru
3.19	Řízení přístupu	Dodavatel je povinen po akceptaci informovat o všech mechanismech v řešení, které umožňují obejití síťové a bezpečnostní infrastruktury (back door), a znemožnit jejich použití.	Plně splňuje	systém neobsahuje back door
4	**Logování**			
4.1	Logování	Všechny bezpečnostní události "podezřelé i bezpečnostního incidentu", výskyty nebo pozorovatelné poruchy v informačním systému nebo komunikační síti, které mohou souviset s důvěrností, integritou nebo dostupností informací, musí být logovány.	Plně splňuje	standardní funkčnost
4.2	Logování	Auditní záznamy musí obsahovat minimálně následující informace (relevantní z nich): • systém, zařízení nebo aplikaci, který záznam vygenerovaly; • identifikátor (uživatelské jméno, ID procesu, IP adresu, terminál, apod.) osoby, programu, služby či zařízení, které je zdrojem zaznamenané události; • datum a čas události; • popis důvodu události (přístup uživatele, systémová chyba apod.); • v případě záznamu o přístupu ještě: - zdroj, ke kterému bylo přistoupeno (informace, aplikace, disk, síť apod.); - typ přístupu (čtení, modifikace, zobrazení ve výpisy, SQL dotaz, smazání apod.); - info autorizovaný/anonymní/neautorizovaný přístup (resp. pokus o přístup); - uživatelské oprávnění; - terminál, nebo systém, ze kterého byl přístup (či pokus o přístup) učiněn.	Plně splňuje	standardní funkčnost, všechny uvedené informace logovány

4.3	Logování	Systémový a/nebo aplikační bezpečnostní log musí zaznamenávat úspěšné i neúspěšné události minimálně v rozsahu: • přihlášení a odhlášení; • informace o změně identity (su / runas apod.); • připojení a odpojení externího zařízení; • informace o spuštění a zastavení služeb/daemonů; • informace o změně systémového data a času; • informace o vypnutí/restartu systému; • správu uživatelských účtů a skupin; • import a export dat; • změny v metodě zabezpečení (včetně změn v nastavení logování); • použitá uživatelská práva.	Plně splňuje	Uvedené události logovány na úrovni aplikace nebo na úrovni prostředí, ve kterém aplikace běží (operační systém, db. server). Systém GINIS disponuje kontrolou změny syst. Času
4.4	Logování	Bezpečnostní log databáze musí zaznamenávat minimálně úspěšné a neúspěšné události v rozsahu: • vytvoření, změna a zrušení uživatelských účtů; • vytvoření, změna a zrušení struktur pro ukládání databázových dat; • vytvoření, změna a zrušení DB objektů; • vytvoření, změna a zrušení tabulek; • vytvoření, změna a zrušení indexů; • export/import databáze (je-li to technicky možné); • přidání, odebrání a změna práv DB rolím a uživatelům; • všechny chyby vztahující se k přístupům k neexistujícím objektům; • přejmenování DB objektů; • přidání, odebrání a změny oprávnění DB účtů; • modifikace dat a konfigurace DB engine (je-li to technicky možné); • všechny neúspěšné pokusy o připojení k DB a, je-li to technicky možné, všechna úspěšná připojení; • vypnutí a zapnutí auditních mechanismů a DB engine.	Plně splňuje	řešeno na úrovni databázového serveru
4.5	Logování	Integrita auditních záznamů musí být garantována, neautorizované smazání logů nebo deaktivace auditního mechanismu nesmí být umožněna. Přístup k logům a mechanismu který je generuje smí být umožněn pouze k tomu autorizovaným osobám.	Plně splňuje	auditní záznamy jsou pravidelně vylévány do externího systému (min. perioda 1 minuta)
4.6	Logování	Auditní záznamy musí být uchovávány minimálně po dobu jednoho roku, nebo dle ustanovení platné legislativy, pokud tato stanoví delší čas. Kratší dobu uchovávání logů lze stanovit pouze v případě vzdáleného logování událostí do centrálního systému pro sběr logů (případně SIEM). Přístup k auditnímu logu musí být (pro oprávněné osoby) snadný a proveditelný v přijatelném časovém období.	Plně splňuje	logy zasílány do nadřazeného systém (syslog, eventlog, SIEM) politika uchovávání podle nadřazenéo systému
4.7	Logování	Čas na všech systémech, které generují auditní záznamy musí být synchronizován proti stejnému zdroji.	Plně splňuje	Využívá služeb domény Active Directory
4.8	Logování	Řešení dodavatele musí podporovat možnost vzdáleného logování do centrálního systému pro sběr logů (případně SIEM). Konkrétní způsob vzdáleného logování bude stanoven v závislosti na kapacitě monitorovacího zařízení a dalších technických podmínkách; preferovány jsou standardní nástroje operačního systému (např. syslog přes TCP).	Plně splňuje	podporován syslog, eventlog, syslog-ng
4.9	Logování	Neúspěšné pokusy o autentizaci musí být logovány.	Plně splňuje	standardní funkčnost
4.10	Logování	Zahájení a ukončení uživatelské relace musí být logováno.	Plně splňuje	standardní funkčnost
4.11	Logování	Řešení musí zaznamenávat všechny akce uživatelů privilegovaných účtů (administrátoři a operátoři s právem konfiguračních změn).	Plně splňuje	standardní funkčnost
4.12	Logování	Všechna zařízení musí být konfigurována tak, aby generovala auditní záznamy o přístupech z konsole.	n/a	nejsou přístupy z konzole
4.13	Logování	Všechna (relevantní) zařízení musí být konfigurována tak, aby generovala auditní záznamy o odepření komunikace IP filtry a/nebo ACL.	Plně splňuje	závisí na nastavení připojujících se zařízení
4.14	Logování	Jsou-li auditní záznamy uloženy lokálně (dočasně či trvale), musí být implementován mechanismus, který zajistí přístup k záznamům pouze k tomu autorizovaným osobám.	Plně splňuje	standardní funkčnost
4.15	Logování	Logy a mechanismy, které je generují nesmí být pod kontrolou uživatelů a administrátorů, jejichž činnost je zdrojem těchto záznamů (v rámci technických možností).	Plně splňuje	logy mohou být odlévány mimo sledovaný systém
4.16	Logování	Auditní mechanismus nesmí dovolit uživatelům a (je-li to technicky možné - např. odesláním logu mimo dosah administrátora) administrátorům modifikovat auditní záznamy.	Plně splňuje	ze záznamů v logu jsou generovány dávky, které jsou odesílány mimo sledovaný systém
4.17	Logování	V případě pokusu o neautorizovaný přístup nebo modifikaci auditních záznamů musí být o této události vygenerován záznam do logu.	Plně splňuje	standardní funkčnost
4.18	Logování	Jednotlivé auditní záznamy musí být automaticky parsovatelné (např. je použit jednoznačný oddělovací znak mezi jednotlivými položkami, nebo pevná délka položek záznamu).	Plně splňuje	záznamy jsou parsovatelné (XML, syslog, zdroj v databázi)
4.19	Logování	Řešení musí být schopné automatické adaptace na změnu času (zimní / letní).	Plně splňuje	standardní funkčnost - v době posunu času o hodinu zpět však není možno systém využívat
5	**Síťová bezpečnost**			
5.1	Síťová bezpečnost	Řešení musí podporovat umístění do oddělených síťových segmentů s filtrovanou komunikací (např. aplikační a DB server v jiných segmentech, komunikace filtrována na firewallu tak, že je dovolena je pouze minimální nezbytná komunikace mezi definovanými IP adresami na definovaných komunikačních portech). Řešení musí splňovat definované požadavky na omezení komunikace mezi síťovými segmenty (minimálně musí být pro veškerou síťovou komunikaci dodána komunikační matice mezi jednotlivými komponentami řešení na úrovni zdrojová/cílová IP adresa + komunikační port).	Plně splňuje	systém využívá serverových aplikací pracujících na standardních síťových protokolech, může pracovat v různých síťových segmentech, komunikaci na firewallech lze omezit pouze na nutné porty
5.2	Síťová bezpečnost	Komunikace mezi jednotlivými síťovými zónami a komunikace přes veřejné sítě musí být šifrována (povolené šifrovací algoritmy a délky šifrovacích klíčů stanoví Vyhláška o kybernetické bezpečnosti č. 82/2018). Je preferováno šifrování na základě certifikátů.	Plně splňuje	standardní aplikace využívají protokol https s využitím certifikátů s dostatečným zabezpečením
5.3	Síťová bezpečnost	Spojení do sítě MD z externích sítí je umožněnou pouze na základě předchozí autentizace a autorizace. Je povolenou pouze spojení pomocí standardní VPN. Všechna spojení mezi sítí MD a externími sítěmi musí být chráněna minimálně firewallem. Použití modemů a podobných komunikačních zařízení (ADSL, WiFi routery apod.) pro propojení externích sítí se sítí MD není dovoleno s výjimkou oběma stranami předem odsouhlasených propojení s definovanou úrovní zabezpečení komunikace.	Plně splňuje	nastavení síťových zařízení a autentizace bude podle požadavků MD dohodnutých ve fázi implementace

5.4	Síťová bezpečnost	Komunikační sítě vytváří bezpečnostní mechanismy a kontroly, které zabrání, zaznamenávají a monitorují hrozby sítě a chrání systémy, které používají síť a informace, které jsou v cestě před těmito hrozbami. Řešení musí splňovat požadavky kladené uvedenými mechanismy, zejména musí být v rámci dokumentace dodán popis veškeré síťové komunikace tak, aby bylo možné tuto komunikaci zadat jako korektní a povolenou.	Plně splňuje	popis komunikačních kanálů bude dodán
6	**Bezpečnost software/aplikací**			
6.1	Bezpečnost software/aplikací	Zranitelnosti, které účinně a systematicky ovlivňují operační systémy, základní software i knihovny použité při vývoji/provozu aplikací, musí být řízeny. Doba vystavení systému riziku jejich zneužití musí být minimalizována. Všechny zranitelnosti musí být ošetřeny do 2 měsíců od vydání oficiální bezpečnostní záplaty, resp. doporučeného postupu pro minimalizaci rizika zneužití.	Plně splňuje	zranitelnosti sledovány, aplikovvány opravy, opraveneé verze doručovány zákazníkovi
6.2	Bezpečnost software/aplikací	Veškeré údaje zadávané do systémů/aplikací musí být validována minimálně z pohledu formální správnosti (má-li být na vstupu číslo, nelze akceptovat písmeno). Systémy a aplikace musí obsahovat interní kontroly validace dat, které budou detekovat jakoukoli korupci informací v důsledku procesních chyb nebo záměrných akcí.	Plně splňuje	pro webové aplikace využívána sanitizace
6.3	Bezpečnost software/aplikací	Při výměně dat mezi systémy a aplikacemi musí být zavedeny mechanismy pro kontrolu integrity a pravosti dat.	Plně splňuje	používán kontrolní součet
6.4	Bezpečnost software/aplikací	Změny v systémech a aplikacích musí probíhat řízeně. Změny v SW balíčcích dodaných výrobce musí být minimalizovány a realizovány standardními postupy (nová verze balíčku, oficiální patch apod.).	Plně splňuje	řízeno interními standardy vývoje založenými na ISO 9000
6.5	Bezpečnost software/aplikací	Veškeré binární soubory, databázové objekty a účty, které se již nepoužívají (ukončení používání aplikačních modulů, knihoven apod.), musí být z aplikace / databáze / operačního systému odstraněny v nejbližším možném termínu. Zdrojové kódy aplikací nesmí být uloženy na provozních systémech.	Plně splňuje	nepotřebné soubory a databázové objekty jsou mazány, nepotřebné účty deaktivovány
6.6	Bezpečnost software/aplikací	Vývojové, testovací a produkční systémy musí být odděleny, aby se snížila rizika související s neoprávněným přístupem nebo změnami softwaru. Přenesení systémů a aplikací mezi vývojovým, testovacím a produkčním prostředím musí být předem schváleno a musí být realizováno definovaným řízeným postupem.	Plně splňuje	závislé na požadavcích zákazníka
6.7	Bezpečnost software/aplikací	Ve vývojovém a testovacím prostředí nesmí být používána provozní data. V pilotním provozu (certifikace nebo předprodukce) nesmí probíhat testování na provozních datech, pokud nelze zaručit stejnou úroveň bezpečnosti jako na produkčním prostředí. I v takovém případě je použití provozních dat možné pouze po předchozím schválení autorizovanou osobou.	Plně splňuje	závislé na požadavcích zákazníka
6.8	Bezpečnost software/aplikací	Automatické odhlášení uživatele (administrátora, …) musí být nastaveno po 15 minutách nečinnosti. Ve zvláštních případech může být u neanonymních autorizovaných účtů nastaveno po předchozím schválení až 60 minut. Pokud by bylo třeba nastavit čas delší než 60 minut musí být tento fakt navíc uveden a zdůvodněn v provozní dokumentaci.	Plně splňuje	automatické odhlášení lze nastavit
7	**Bezpečnost databází**			
7.1	Bezpečnost databází	Přístup k DB objektům, rolím, roli DBA, rolím aplikačních administrátorů, uživatelů a vývojářů. • Každý koncový uživatel musí mít přístup k daným objektům databáze prostřednictvím rolí určených pro danou aplikaci. Role musí být založeny na funkcích prováděných aplikacemi. Oprávnění k objektům mohou být přidělena přímo jednotlivým databázových účtům pouze na základě udělení výjimky. Oprávnění k objektům nesmí být přidělena roli PUBLIC (pokud není výslovně požadováno dodavatelem databáze). Přístup k pohledům a tabulkám umožňující přístup k informacím z celé DB musí být omezen pouze na správce databáze nebo automatizované účty, které jsou uvedeny v provozní dokumentaci. Je možné, že některé aplikace vyžadují přístup pouze ke čtení na části těchto dat. Pokud tomu tak je, musí to být uvedeno v provozní dokumentaci; • Role umožňují definování a přidělování oprávnění k databázi aplikačním funkcím. Individuálně požadovaná oprávnění a další role databáze musí být přiděleny pouze databázové roli, která pak umožňuje přidělování nebo odebrání oprávnění databázovým účtům (příkladem takových rolí mohou být role DBA, role administrátorů aplikací a specifické role koncových uživatelů). Uživatelé mohou mít přiděleny pouze role, které umožňují výkon specifických funkcí odpovídajících jejich pracovní náplni. Role PUBLIC nesmí být přidělena. Přístupová práva nesmí být přidělena přímo účtům koncových uživatelů s výjimkou účtů vytvořených implicitně při instalaci pro údržbu databázového systému (v souladu s instalačními postupy) a účtu v databázi, která má pouze jeden, tedy uživatelský, účet. Pokud je nutné přidělit přístupová práva k DB objektům přímo aplikacím, musí být tato skutečnost popsána a zdůvodněna v provozní dokumentaci. • Role DBA obsahuje všechna systémová oprávnění databáze, má úplný přístup k datovému slovníku databáze. V provozním prostředí smí být role DBA přiřazena výhradně účtům autorizovaných správců databází. Ve vývojovém a testovacím prostředí smí být role DBA přidělena správcům účtů databáze a účtům autorizovaných vývojářů aplikací. • Role administrátora aplikace umožňuje přidělování oprávnění uživatelským účtům umožňujícím určitý typ správy aplikace odlišný od účtů DBA. Tato oprávnění mohou například zahrnovat vytváření účtů uživatelských aplikací, vytváření profilů účtů a přidělování oprávnění těmto účtům. Role administrátora aplikace smí být aktivována pouze konkrétní databázovou aplikací nebo heslem chráněnou vloženou procedurou. Role administrátora aplikace nesmí být použita jako implicitní role pro koncové uživatele. • Každá aplikace definuje různé role, které obsahují všechna oprávnění nezbytná pro uživatele aplikací a zvláštní roli administrátora aplikace. Při vytváření účtu uživatele aplikace je tomuto účtu přidělena odpovídající role. Žádná z aplikačních rolí nesmí být přiřazena jako implicitní, je tedy nutné, aby aplikace každou roli přidělila definovaným způsobem. Jednomu uživateli může být v závislosti na jeho pracovní náplni přiděleno více rolí. Žádný uživatelský účet nesmí mít právo měnit nastavení jiného uživatelského účtu. Žádný uživatelský účet nesmí mít přístup k tabulkám DBA, pohledům (views) a dalším objektům DBA. Pokud aplikace vyžaduje přístup k určitým položkám takových údajů, musí to být uvedeno v provozní dokumentaci a schváleno jako výjimka • Role vývojáře aplikací se používá k přidělování oprávnění účtům vývojářů aplikací. Software, logy, datové soubory a další adresáře a soubory databáze v produkčním prostředí nesmí být vývojářům přístupné. V produkční databázi nesmí být účty pro vývoj aplikací. V ideálním případě vývojáři nemají oprávnění DBA ani ve vývojovém/testovacím prostředí. Všechny vývojové účty a odpovídající objekty DB musí být chráněny před ostatními vývojovými účty. Ve vývojové/testovací databázi musí být též vytvořen účet vlastníka aplikace (a vlastníka jejích objektů) a vývojáři musí zpřístupnit majiteli tohoto účtu lokálně testované objekty. Pokud je nastavení takového systému problematické (vývoj je řízen jednou osobou, která je také správcem aplikace), je nutné zajistit, aby aplikace byla testována na účtu, který nemá oprávnění DBA (nebo z pohledu oprávnění, odpovídá provoznímu účtu/prostředí)..	Plně splňuje	Uživatel systému GINIS nemá práva pro přístup k datům aplikace - má přiřazena pouze práva pro spuštění incializační procedury . Po provedení autentizační procedury a ověření uživatele je uživatel aplikačně relogován na účet silného uživatele (s právy nižšími než DBA), pod kterým jsou prováděny aktivní operace . Role s vyššími právy je využívána pouze pro úpravy datových struktur při upgradech aplikace na vyšší verzi či při rozšiřování systému o nové subsystémy, které jsou prováděny specializovanými aplikacemi.
7.2	Bezpečnost databází	Účty správce databáze jsou určeny pro správu dat, definování oprávnění, správu a sledování databázových objektů, konfiguraci databáze a pro spouštění a vypínání databáze. • Tyto privilegované účty smí sloužit pouze pro správu databáze a nesmí se používat pro vývoj, testování nebo provoz aplikací; • Všechny účty správců databáze musí být neustále chráněny silným heslem; je zakázáno používat defaultní hesla; • Účty správce databáze nesmí být sdíleny více uživateli; každý správce musí pro správu databáze používat individuální účet s oprávněními správce; • Účty operačního systému s udělenými oprávněními administrátora databáze musí být přiděleny výhradně jednotlivě (nesmí být sdíleny).	Plně splňuje	Privilegované účty pro správu oper. systému a databázového serveru jsou poskytovány zákazníkem a spolu s ním řízeny. Nejsou potřebné pro běh či správu aplikace.

7.3	Bezpečnost databází	Vlastnictví objektu zajišťuje plný přístup k danému objektu. Všechny databázové objekty musí být vlastněny databázovým systémem, správcem databáze nebo účty vytvořenými speciálně pro vlastnictví aplikačních objektů. • Pro každou aplikaci musí být vytvořen speciální účet (případně účty), který bude vlastnit všechny objekty dané aplikace; • Koncový uživatel nesmí vlastnit žádné databázové objekty; • Pouze správce aplikace smí mít možnost přidělit oprávnění objektům jednotlivým aplikačním rolím; • Uživatel nesmí mít možnost přihlášení k účtu, který je vlastníkem aplikačního objektu. Účet, který je vlastníkem aplikačních objektů, smí být používán pouze pro správu těchto objektů. Pokud se účet vlastníka aplikace nepoužívá, musí být uzamčen; • Defaultní DB účty nesmí být používány jako účty vlastnící aplikační objekty nebo schémata.	Plně splňuje	Pro vlastnictví všech db. objekků aplikace je určen jediný účet založený k tomuto účelu. Práva k aplikačním rolím jsou spravována prostřednictvím aplikace GINIS ADM. Uživatel nemá možnost přímo přistupovat k db. objektům aplikace - přistupuje pouze prostřednictvním aplikace.
7.4	Bezpečnost databází	Uživatelské účty slouží k přístupu k databázovým objektům aplikace prostřednictvím funkcí aplikace. • Uživatelům jsou přidělována pouze ta oprávnění (role), která potřebují pro výkon své pracovní činnosti, a jsou to pouze ta, která umožňují uživateli provádět definované operace; • Jednotlivá oprávnění nesmí být přidělena přímo koncovým uživatelským účtům; oprávnění musí být přidělena uživatelským účtům prostřednictvím databázových rolí.	Plně splňuje	Uživatel nemá možnost přímo přistupovat k db. objektům aplikace - přistupuje pouze prostřednictvním aplikace.
7.5	Bezpečnost databází	V případě použití vícevrstvé architektury je pro přístup k DB využíván pouze jeden účet (pro aplikační server); bezpečnost takového účtu závisí na úrovni zabezpečení síťové komunikace a autentizačních metodách mezi aplikační a databázovou vrstvou. Logování na úrovni jednotlivých uživatelů pak není v rámci DB možné. V takovém případě: • logování akcí uživatelů musí být detailně řešeno na aplikační úrovni; • přístup k výše uvedenému speciálnímu účtu misí být omezen pouze pro server vyšší (aplikační) vrstvy na úrovni konfigurace sítě a použitím silných autentizačních metod; • způsob auditu uživatelských akcí musí být detailně popsán v dodané dokumentaci.	Plně splňuje	Při provozu webových aplikací (vícevrstvá architektura) je pro přístup k datům používán jediný účet (s právy nižšími než DBA). Akce uživatelů mohou být logovány.
7.6	Bezpečnost databází	Zásadním nedostatkem použití aplikačních účtů k DB je nutnost uložení autentizačních údajů na aplikačním serveru, proto: • je-li to technicky možné, musí být použita autentizace pomocí aplikačního certifikátu; • jména a hesla uložená na aplikačním vrstvě musí být šifrována, nebo chráněna jiným odpovídajícím mechanismem; • tyto účty nesmí být používány (sdíleny) interaktivními uživateli; • je-li to technicky možné, musí být přístup k těmto účtům omezen na definovanou dobu; • v případě použití ověření pomocí účtu operačního systému, nesmí být k takovému účtu umožněn vzdálený přístup a veškeré použití takového účtu musí být logováno i na úrovni operačního systému.	Plně splňuje	Heslo aplikačního účtu k DB je uloženo v šifrované podobě.
7.7	Bezpečnost databází	Identifikátory instancí, adresy sítí a názvy počítačů / instance (názvy hostitelů) mohou pomoci hackerům, kteří vyhledávají a získají přístup k databázi. Tyto informace nesmějí být dostupné z veřejných zdrojů (e-mailové konference, news groups a další komunikační platformy, sociální sítě, externí webové servery apod.), a vždy musí být chráněny před neoprávněným přístupem. Informace o konkrétních databázích musí být přístupné pouze oprávněným uživatelům a nesmí být distribuovány mezi dalšími uživateli sítě.	Plně splňuje	závislé na implementaci a bezpečnostní politice zákazníka
7.8	Bezpečnost databází	ODBC, JDBC: • Autorizace pro databázové objekty přístupné prostřednictvím ODBC musí být definovány v databázi a nikoliv pouze v aplikaci; • Funkce sledování ODBC musí být v operačním prostředí zakázána, protože je nezbytné zabránit ukládání citlivých dat do souborů na disku; • Připojení ODBC musí používat pouze oprávnění definovaná na úrovni databázového systému; • Hesla pro databázové účty nesmí být uložena v otevřené podobě v definovaném připojení ODBC nebo DSN (data set names);. • JDBC: Informace o připojení, zejména heslech databázových účtů, nesmí být přístupné v otevřené podobě; WEB Server, střední vrstva: • Architektura sítě mezi aplikačním serverem a databází musí vycházet z klasifikace přenášených dat a požadavky na přístup; • Pokud jsou servery aplikačních a DB serverů provozovány odděleně, musí být komunikace mezi nimi šifrována; • Přenášená ověřovací data musí být vždy šifrována.	n/a	ODBC přístup není použit
7.9	Bezpečnost databází	• Pro účely replikace musí být použity různé účty pro správce replikace a pro databázové účty replikovaných systémů; • Hesla účtů musí být během přenosu po síti šifrována; • Přístup k replikačním procedurám musí být omezen pouze na správce příslušné databáze a replikačních účtů; • Replikovaná data mohou být dočasně uložena v oblastech operačního systému určeného pro tento účel. Tato data musí být přístupná pouze komponentám replikačního systému. Správa přístupů se provádí konfigurací příslušných přístupových práv operačního systému a databáze; • Struktura a konfigurace replikačního systému musí být podrobně popsána v dodané dokumentaci.	Plně splňuje	V případě replikací jsou hesla účtů při přenosu šifrována a přístup k replikačním mechanismům je řízen.
7.10	Bezpečnost databází	• Autentizace mezi propojenými databázemi může být provedena pomocí autentizačních údajů DB session, která vytvoří propojení, nebo pomocí speciálních uživatelských jmen a hesel. Je preferováno použití autentizačních údajů daného uživatele (získaných například z některé z adresářových služeb), protože umožňuje jednoduché a logovatelné řízení správy identit v celé síti; • Pokud databáze sdílí data pomocí síťového DB linku, musí databáze inicializující propojení používat autentizační data aktuální DB session; • Přístup k DB linku musí být omezen pouze na oprávněné uživatele (je-li to technicky možné); • Aplikace nesmí vytvářet a používat veřejné odkazy na databázi. Je-li použití veřejných vazeb technicky nezbytné, musí být v provozní dokumentaci detailně popsáno a zdůvodněno; • Databázová propojení nesmí být definována mezi provozními a testovacími/vývojovými databázemi.	n/a	nepředpokládá se využití propojených databází. V případě jejich použití bude aplikace splňovat uvedené požadavky
8	**Bezpečnost webových aplikací**			

8.1	Bezpečnost webových aplikací	Identifikace a autentizace: • Přístup ke zdrojům (stránky, soubory apod.) musí být podmíněn autentizací s výjimkou takových, které jsou deklarovány jako veřejné; Konkrétně přístup k osobním údajům: - bude umožněn pouze uživatelům, kteří byli jednoznačně identifikováni a ověřeni; - uživatelé musí být jednoznačně identifikováni a ověřeni aplikací, není povolen přístup generických (defaultních) uživatelů a sdílených účtů; • Všechncy autentizační mechanismy musí být implementovány na straně serveru; • Všechny autentizační mechanismy musí pracovat s chybami bezpečným způsobem (zachytávání, bezpečná správa výjimek apod.); • Aplikace musí uživatelům kdykoliv umožnit bezpečnou změnu autentizačních údajů; • Pole pro hesla nesmí zobrazovat znaky prostého textu (např. je nahrazují hvězdičkou), funkce autocomplete nesmí být povolena; • Mechanismy pro helsa musí být nastaveny tak, aby splňovaly požadavky BPI MD (včetně příloh, zejména "Pravidla pro provozovatele"); • Pokusy o přístup k aplikaci (úspěšné i neúspěšné) musí být logovány; • Hesla nesmí být ukládána v prostém textu, pouze jejich hashe. K heslům (jejich hashům) smí přistupovat pouze autentizační modul aplikace s omezeným přístupem; • Veškerý kód, který implementuje nebo používá autentizační mechanismy nesmí být ovlivnitelný škodlivým kódem (malicious code); • Pokud při autentizačním procesu uživatel překročí definovaným maximální počet neúspěšných pokusů o přihlašování, musí být účet zablokován (viz. příloha BPI "Pravidla pro provozovatele"); • Aplikace musí zajistit bezpečný mechanismus obnovení zapomenutých hesel. Tzv. "bezpečnostní otázky" nejsou povoleny.	Plně splňuje	Pro správu hesel předpokládáme využití autentizačních mechanizmů ActiveDirectory/LDAP. Kde zejména AD má silnou podporu politik nastavování hesel. • Aplikace je koncipována jako Single Page - t.j. všechny prvky jsou přenášeny přes jeden obslužný bod, který vyžaduje ověření uživatele • Autentizace/autorizace probíhá na serveru • Správa vyjímek je parametrizovaná, bude v režimu zobrazení identifikátoru, nikoliv detailů • Aplikace bude nastavena do módu, kdy ověřování bude probíhat oproti AD, nikoliv databázi • Aplikace není ovlivněna škodlivým kódem známým v době podání nabídky • Zablokování účtu je součástí politiky hesel AD
8.2	Bezpečnost webových aplikací	Řízení přístupu: • Uživatelé smí mít přístup pouze k funkcím, odkazům, službám, zdrojům a informacím pro které mají definovaná přístupová oprávnění; musí být použit princip "nutně potřebuje znát ke své práci“; • Všechny přímé odkazy na interní objekty (soubory, adresáře, záznamy databáze ...) musí být řádně chráněny; • Prohlížení adresářů (directory listing/browsing) je zakázáno (kromě případů, kdy je to vyžadováno); • Koncovým uživatelům nesmí být umožněno měnit polituty a uživatelské atributy používané pro řízení přístupu; • Aplikace nesmí uživatelům umožnit obejití/přeskočení omezení přístupu k aplikacím plynoucí z interních procesů (např. denní limity transakcí nebo úkoly pracovního postupu); • Veškeré mechanismy řízení přístupu musí být implmentovány na strane serveru; • Aplikace musí umožit implementaci procesu registrace, úpravy a zrušení registrace uživatelských oprávnění k aplikaci; doporučuje se vytvořit uživatelský profil a/nebo zásady řízení přístupu založené na uživatelských rolích; • Aplikace musí umožit aktualizovat seznam uživatelů a rolí / profilů a oprávněných přístupů pro každou z nich; • Aplikace musí umožit implementaci procesu přidělování, distribuce, ukládání, vypršení platnosti a formát hesel tak, aby byla zajištěna jejich důvěrnost a celistvost; • Přístup do administračního a řídicího modulu aplikace musí mít minimálně stejnou úroveň zabezpečení jako přístup do modulu uživatele; • Aplikace nesmí uživatelům zobrazovat funkce a volby, ke kterým uživatel nemá přístupová oprávnění; • Veškeré mechanismy řízení přístupu musí pracovat s chybami bezpečným způsobem (zachytávání, bezpečná správa výjimek apod.); • Veškerý kód, který implementuje nebo používá mechanismy řízení přístupu nesmí být ovlivnitelný škodlivým kódem (malicious code); • Pokusy o přístup k funkcím/modulům a datům aplikace (úspěšné i neúspěšné) musí být logovány; • Pokud má webová aplikace přístup k databázi, musí být implementována prostřednictvím jednoho nebo více DB účtů s omezeným oprávněním bez možnosti úpravy schématu DB; • Přístup k databázi musí být implementován pomocí uložených procedur (parametrizován) z důvodu možnosti odmítnutí přístupu; přístup musí být realizován prostřednictvím DB účtu s nízkým oprávněním.	Plně splňuje	• Aplikace nevystavují interní odkazy - ja SPA aplikace přistupují přes jeden bod • Prohlížení je zakázáno • Uživatel je přihlášen jako referent a v aplikaci nemůže ovlivňovat své zařazení - je dáno administrací systému • Přístup do administračního modulu je vázán stejnými pravidly jako přístup do ostatních modulů • Přístup k databázi je zajištěn pomocí relativně omezného uživatele. • Pouze při servisních akcích(povýšení databáze) je použit uživatel s vyšším oprávněním

8.3	Bezpečnost webových aplikací	Session management: • Aplikace musí používat session control poskytované výchozím prostředím; • Session ID uživatele musí být po úspěšném přihlášení změněno; • Session ID se musí měnit a být odlišné pro každé přihlášení a/nebo opětovnou autentizaci; • Ukončí-li uživatel práci s aplikací, musí být uživatelská session zrušena; • Session ID musí být zrušeno po procesu "odhlášení"; • Přístup ke cookie obsahující session ID musí být omezen; • Parametry obsahující session ID musí mít nastavené parametry pro bezpečný přenos HTTP a pro zamezení ukládání v cashi; • Veškerý kód, který implementuje nebo používá session management nesmí být ovlivnitelný škodlivým kódem (malicious code); • Musí být implementován mechanismus pro automatické odhlášení uživatele při nečinnosti delší než 30 minut (doporučuje se použít časový interval 15 minut); • Session token relace musí být dostatečně dlouhý a náhodný, aby odolal běžným útokům na nasazené aplikační prostředí; • Pro kritické aplikace (aplikace zpracovávající extrémně citlivá data) musí být session ID měněno po uplynutí definovaného časového úseku nebo po definovaném počtu požadavků; použití tohoto mechanismu je doporučeno pro všechny aplikace pracující s neveřejnými daty; • Všechny stránky, ke kterým přistupují autentizovaní uživatelé, musí mít možnost odhlášení; • Session ID nesmí být zobrazeno v URL, chybových zprávách nebo protokolech, s výjimkou záhlaví souborů cookie; aplikace nesmí umožnit přepisování session cookies a URL.	Plně splňuje	• Použita je ASP.NET technologie SessionID, která splňuje požadavky pro přihlášení/změnu a pod. • Administračně lze nastavit plovoucí prodlužování platnosti, nebo ukončení session po uplynutí stanovené doby • Problematická je změna session id v průběhu práce • Možnost odlášení uživatele je samozřejmost
8.4	Bezpečnost webových aplikací	Ověření vstupů: • Runtime enviroment nesmí být náchylné k přetečení vyrovnávací paměti (buffer overflow) prostřednictvím použití mechanismů definovaných technikami pro bezpečné programování; • Všechny vstupy dat musí být prověřovány na formální správnost (například délky řetězců, použití písmen tam, kde má být číslo apod.); • Všechny chyby při validaci vstupních dat musí mít za následek odmítnutí těchto dat nebo jejich zadání v povoleném formátu; • Všechna ověření vstupů musí být implementována na straně serveru (je povoleno, aby některá ověření na straně serveru bylo možné provést redundantně i na straně klienta, například pomocí JavaScriptu); • Veškeré formy zadávání údajů neautentizovanými uživateli musí být zajištěny použitím "captcha" nebo obdobným mechanismem, který zabraňuje zneužití formulářů automaty; • Znakové sady musí být stejné (např. UTF-8) pro všechny vstupní zdroje aplikace; • Aplikace musí použít ověření formální správnosti pro každý jednotlivý vstup dat; • Veškerý kód, který implementuje nebo používá mechanismy validace vstupních dat nesmí být ovlivnitelný škodlivým kódem (malicious code); • Veškeré negativní validace vstupních dat musí být logovány; • Veškerá vstupní data musí být před validací kanonizována.	Částečně splňuje	• moduly založené na .NET splňují • technologie ASP.NET zabraňuje buffer overflow z principu - neměnnost řetězců, managed heap • formální správnost dat na klientské straně zajišťuje formulářový systém • na klientské straně nedoporučujeme logování chybných dat
8.5	Bezpečnost webových aplikací	Ověření výstupů: • Data vytvářející HTML výstupy (prvky HTML, atributy HTML, hodnoty jazyka JavaScript, bloky CSS a atributy adresy URL), jsou v použitém kontextu řádně překódována (konverze speciálních znaků); • Veškerý kód, který implementuje nebo používá mechanismy kontroly výstupů musí být implementován na straně serveru; • Všechna data odeslaná do SQL interpreteru musí používat parametrizovaná rozhraní nebo předpřipravené příkazy/dotazy nebo být vhodně překódována (konverze speciálních znaků); • Všechny znaky, které nejsou pro intepreter známé, musí být překódovány; • Data zaslaná libovolnému interpreteru musí být prověřena/překódována, zejména: - Všechna data odesílaná přes rozhraní XML musí použít parametrizované rozhraní nebo být vhodně překódována; - Veškerá data použitá v spojeních LDAP musí být vhodně překódováva; - Data používaná jako parametry příkazů operačního systému musí být řádně překódováva; • Veškerý kód, který implementuje nebo používá mechanismy validace výstupních dat nesmí být ovlivnitelný škodlivým kódem (malicious code).	Plně splňuje	• server vytváří data a zasílá je klientovi. Tím je zajištěno jednotné ošetření speciálních znaků. • serverová strana pracuje pomocí přednastavených SQL příkazů v aplikačním serveru • LDAP konektory standardně pracují v UTF-8 • SQL dotazy se skládají na straně aplikačního serveru, nikoliv na klientovi

8.6	Bezpečnost webových aplikací	Bezpečnost komunikace: • SSL/TLS musí být použito pro všechna připojení, která: - vyžadují autentizaci uživatele; - souvisejí s procesem změny hesla; - odesílají nebo přijímají data/citlivé funkce; - souvisí se správou aplikace; • Všechna připojení k externím systémům zahrnujícím výměnu dat/citlivé funkce musí být autentizována; • Všechna připojení k externím systémům s funkcí výměny dat/citlivých funkcí musí používat účet s nastavenými minimálními potřebnými oprávněními; • Všechny autentizační údaje k externím systémům a aplikacím musí být uloženy šifrovaně v úložišti s omezeným přístupem (nikoliv ve zdrojovém kódu); • SSL certifikáty používané servery musí být podepsané certifikačními autoritami rozpoznatelné prohlížeči tak, aby uživatelům umožnily přístup k aplikaci; • Chyby v SSL spojení nesmí umožnit nezabezpečené spojení; • Chyby v SSL spojení musí být logovány; • Musí být definována jednotná znaková sada (např. UTF-8) pro všechna spojení; • Přenos citlivých dat a/nebo osobních údajů musí být šifrován.	Plně splňuje	• zde splnění požadovaných podmínek závisí hlavně na administraci systému a implementaci • doporučujeme nasadit SSL(https) i v rámci intranetu • systém pracuje s certifikáty standardnímn způsobem, takže závisí na bezpečnostní politice, zda budou použity certifikáty vystavené organizací, nebo nakoupené
8.7	Bezpečnost webových aplikací	Kryptografie: • Všechny kryptografické funkce pro ochranu citlivých informací v rámci aplikace musí být implementovány na straně serveru; • Všechny vygenerované hashe pro ukládání hesel musí mít přidánu "sůl" (řetězec dostatečné délky pro zabránění útokům slovníku nebo hrubou silou); • Všechny kryptografické moduly a certifikáty musí mít ošetřeno bezpečné zpracování chyb; • Přístup k libovolnému hlavnímu klíči (master key) musí být chráněn před neoprávněným přístupem (hlavní klíč jsou přístupové údaje aplikace uložené na disku a slouží k ochraně přístupu k informacím o konfiguraci zabezpečení); • Všechna čísla, názvy souborů, identifikátory nebo náhodně generované řetězce musí používat kryptografické moduly ověřené dle uznávaných standardů tak, aby tyto hodnoty nemohly být útočníkem uhádnuty; • Veškerý kód, který implementuje nebo používá kryptografický modul nesmí být ovlivnitelný škodlivým kódem (malicious code); • Kryptografické moduly používané aplikací byly ověřeny dle standardu FIPS 140-2 nebo ekvivalentním: http://csrc.nist.gov/groups/STM/cmvp/validation.html; • Aplikace musí umožnit implementaci procesu ověření identity/el. podpisu dle Nařízení EU 910/2014 (eIDAS).	Částečně splňuje	• Ano, aplikace používá kryptografické funkce na straně serveru • Aplikace používá standardních kryptografických prostředků windows • Kryptografická sůl je přidávána, nicméně uložení hesel je předpokládáno v doméně • Jsme eidas compatible
8.8	Bezpečnost webových aplikací	Chyby a logování: • Aplikace musí ukládat do auditního protokolu (logu) minimálně: - informace o aktivitách administrátorů aplikace; - události související s bezpečností aplikace; - úspěšné i neúspěšné pokusy o autentizaci; - přístupy autentizovaných i neautentizovaných uživatelů; - události související s provozem a správou systému; - chyby systému; - změny v přístupových oprávněních (navýšení/snížení práv, změny v uživatelském profilu apod.); - zapnutí/vypnutí a změny v auditním mechanismu; - chyby v SSL; • Chybové zprávy vygenerované aplikací nesmí obsahovat citlivá data, která mohou útočníkovi pomoci v jeho činnosti (např. ID relace, osobní údaje apod.); • Všechny mechanismy týkající se zpracování chyb a logování musí být implementovány na straně serveru; • Výchozí nastavení pro přístup k funkcím správy a auditnímu protokolu (včetně nastavení) musí být odmítnutí přístupu; • Veškerý kód, který implementuje nebo používá mechanismy pro zpracování chyb a logování nesmí být ovlivnitelný škodlivým kódem (malicious code); • Aplikace musí zajistit integritu protokolů auditu a mechanismů, které je generují a odstraňují, proti neoprávněnému přístupu a/nebo deaktivaci; • Přístup k auditním záznamům a kontrola mechanismů, které je generují, smí být umožněn pouze oprávněným osobám. V žádném případě nesmí být mechanismy a protokoly auditu pod přímou kontrolou uživatelů a správců (je-li to pro vykonávání práce uživatelů užitečné/nutné, mohou jim být vybrané záznamy zpřístupněny pro čtení pomocí k tomu určené funkce aplikace); • Aplikace musí podporovat možnost vzdáleného logování do centrálního úložiště logů; • Každý záznam v logu musí obsahovat alespoň následující informace: - datum a čas, kdy k události došlo; - závažnost (severity) události; - identifikátor (přihlašovací jméno uživatele, ID procesu, adresa IP, terminál atd.) osoby, programu nebo komponenty, která způsobila zaznamenání události; - Popis události nebo důvod zaznamu: přístup, došlo k chybě apod.; - Jedná-li se o záznam o přístupu: zdroj, ke kterému bylo přistupováno (informace, aplikace, síť, disk atd.), typ přístupu (čtení, úprava, prohlížení, seznam, smazání atd.), informaci, zda	Plně splňuje	Aplikace používá několika logovacích vrstev. Je věcí implementace, jaká bude použita.
8.9	Bezpečnost webových aplikací	Ochrana citlivých dat • Pro všechny formuláře obsahující citlivé informace je zakázáno ukládání do mezipaměti (cache) na straně klienta, včetně funkcí automatického dokončování vkládaných řetězců/dat; • Všechna citlivá data musí být na server odesílána v těle HTTP zprávy (např. parametry URL se nikdy nesmí používat k odesílání citlivých dat); • Všechna citlivá data (včetně dat dočasně uložených, cache apod.) odeslaná klientovi musí být chráněna před neoprávněným přístupem nebo musí být uložení znemožněno (např. nastavit záhlaví s parametrem "no cache") a/nebo jsou data po ukončení relace uživatele nevalidní; • S osobními údaji musí aplikace nakládat tak, aby bylo možné zajistit fungování procesů pro zajištění práv subjektů údajů dle Nařízení EU 2016/679 (GDPR).	Plně splňuje	• Aplikace splňuje GDPR a záleží na implementaci jak bude použita • Aplikace nekomunikuje pomocí url parametrů(pouze minimálně technologicky, nikoliv ve smyslu přenášení formulářových dat).

8.10	Bezpečnost webových aplikací	HTTP Security • Aplikace smí přijímat pouze definovanou omezenou sadu metod (např. pouze GET a POST); • V HTTP hlavičce musí být vždy uveden typ obsahu (parametr "content type") uvedením bezpečné znakové sady (např. UTF-8); • Příznak "HTTPOnly" musí být nastaven ve všech souborech cookie, které explicitně nevyžadují specifický přístup z jazyka JavaScript (takové je třeba uvést v dokumentaci); • Příznak "Secure" musí být použit ve všech souborech cookie, které obsahují citlivá data, včetně session cookie; • HTTP hlavičky smí obsahovat pouze znaky ASCII (platí pro data posílaná aplikacích i pro uživatelské odezvy); • Aplikace musí generovat dostatečně náhodný token (např. Captcha) jako součást všech odkazů a formulářů, které slouží pro anonymní vstup dat a/nebo jsou spojeny s transakcemi s citlivými daty. Aplikace musí zkontrolovat tento token s odpovídající hodnotou pro uživatele, který provádí požadavek, před zpracováním takto zadaných dat.	Plně splňuje	• Aplikace podporuje pouze GET a POST • Aplikace podporuje captcha pro anonymní vstup dat • Předpokládáme využití google reCaptcha
8.11	Bezpečnost webových aplikací	Další požadavky • Aplikace musí být schopna zvládnout chybějící, nadbytečné nebo přejmenované parametry (např. korektně zahlásit chybu); • Skrytá pole ("hidden files") smí být použita pouze pro sekvencování stránek; nikdy nesmí být použita pro přenos dat; • Logika aplikace musí být imunní proti pokusům o její obcházení (např. změna pořadí kroků, obcházení kroků apod.); • Aplikace nesmí obsahovat/zobrazovat žádné informace, které by útočníkovi pomohly k plánování/realizaci útoku; • Aplikace musí podporovat sledování uživatelů pomocí dotazů SQL (SQL query user tracking), tedy který uživatel webu provedl v SQL dotaz.	Plně splňuje	• Aplikace minimalizuje používání Url parametrů právě z důvodu bezpečnosti. • Aplikace minimalizuje vystavování informací na nezbytně nutné, nicméně každá zobrazená informace je určitým vodítkem pro útočníka.
9	**Zálohování a business continuity**			
9.1	Zálohování a business continuity	V rámci řešení musí být vytvořeny a dodány havarijní plány a plány obnovy systému/aplikace (nebo jejich částí) po havárii popisující postup řízení případného incidentu/havárie a způsob obnovy činnosti v případě událostí, které mohou ovlivnit její kontinuitu.	Plně splňuje	Havarijní plány budou dodány
9.2	Zálohování a business continuity	Havarijní plány a plány obnovy musí být v rámci akceptace otestovány.	Plně splňuje	Havarijní plány budou otestovány
9.3	Zálohování a business continuity	V rámci řešení musí být vytvořena a implementována strategie zálohování (definice úplných a inkrementálních záloh, manipulace se záložními médii apod.). Zálohovací strategie musí být v rámci akceptace otestována (včetně úplné obnovy systému ze záloh).	Plně splňuje	Bude vytvořena strategie zálohování
9.4	Zálohování a business continuity	Všechny prvky řešení musí mít definované postupy pro zálohy všech součástí – software, konfigurace i data.	Plně splňuje	Budou definovány zálohovací postupy
10	**Legal compliance**			
10.1	Legal compliance	Veškeré informace musí být zpracovávány v souladu s právními požadavky na zabezpečení informací, zejména se: • zákonem 181/2014 sb. ve znění pozdějších předpisů včetně navazujících vyhlášek, zejména vyhláškou 82/2018 sb.; • zákonem 101/2000 sb. ve znění pozdějších předpisů; • nařízením EU 2016/679 (GDPR); • nařízením EU 910/2014 (eIDAS).	Plně splňuje	Aplikace splňuje požadavky uvedených právních předpisů
10.2	Legal compliance	Vytvoření, zabezpečení a uchování logů komunikačních sítí a informačních systémů splnit všechny platné právní požadavky.	Plně splňuje	logy vytvářeny v souladu s bezp. požadavky
10.3	Legal compliance	Použití softwaru, produktů a materiálů chráněných právy duševního vlastnictví bude v souladu s omezeními stanovenými v příslušných právních předpisech a licenčních smlouvách. Jakýkoli software nebo materiál vytvořený pro MD bude dodán včetně příslušných oprávnění pro nakládání a správu tohoto vlastnictví. Veškeré zdrojové kódy zakázkově vyvinutého SW budou vlastnictvím MD.	Plně splňuje	SW je vyvíjen a dodáván v souladu s licenčními smlouvami.
10.4	Legal compliance	Postupy, procedury a procesy pro zpracování osobních údajů budou odpovídat všem požadavkům platných právních předpisů a smluv a veškerá opatření budou stanovena v souladu s úrovní zabezpečení informací.	Plně splňuje	Práce s osobními údaji v aplikaci splňuje požadavky na ně kladené ve výše uvedených předpisech
11	**Testování a akceptace**			
11.1	Testování a akceptace	Bezpečnostní testy řešení musí být provedeny před finální akceptací. Tyto testy musí obsahovat minimálně: • scan zranitelností OS/DB/aplikací; • bezpečnostní scan webových aplikací. Případné nalezené zranitelnosti musí být odstraněny před finální akceptací řešení.	Plně splňuje	bezpečnostní testy budou provedeny
11.2	Testování a akceptace	Pro akceptaci nových (resp. upgradů a změn stávajících) systémů/aplikací musí být splněny minimálně následující podmínky: • předaná dokumentace včetně bezpečnostní specifikace, havarijních plánů a plánů obnovy je akceptována; • je akceptován bezpečnostní model (domluvené/stanovené bezpečnostní požadavky); • úspěšné provozní testy; • úspěšné bezpečnostní testy; • úspěšné testy zálohování; • školení uživatelů i obsluhy (je-li potřebné/účelné – rozhodují administrátoři, resp. uživatelé); • další podmínky specifikované v zadání či řízené dokumentaci.	Plně splňuje	provedení uvedených procedur bude podmínkou akceptace
12	**Řízení software**			
12.1	Řízení software	Řešení musí umožnit vypnutí nepoužívaných služeb/daemonů.	Plně splňuje	nepoužívané služby je možno vypnout
12.2	Řízení software	Každý klientský SW určený k práci nebo správě řešení musí být zabezpečený; pokud je založen na platformách třetích stran (např. Java, Flash apod.), musí být kompatibilní s novými verzemi těchto platforem, aby se zabránilo narušení bezpečnosti díky chybám v nich odhalených.	Plně splňuje	Dodávaný SW je kontrolován před distribucí dvěma antivirovými systémy. Kompatibilita s komponentami třetích stran je řízena podle aktuálního GINIS Compatibility listu
12.3	Řízení software	Řešení musí disponovat mechanismem, který zajistí integritu souborů a bezpečnostních záplat operačního systému a aktualizací softwaru. Řešení tedy musí mít všechny známé bezpečnostní zranitelnosti opraveny nebo přezkoumány a akceptovány před instalací provozního prostředí.	Plně splňuje	Integrita dodávaných SW modulů je chráněna kontrolním součtem

12.4	Řízení software	Řešení musí disponovat mechanismy pro odhalení nesrovnalostí/chyb v konfiguraci a při jejich detekci vyvolat alarm. Tato verifikace (a případný alarm) musí být provedena předtím, než se konfigurace stane aktivní.	Plně splňuje	Administrační aplikace aktivně brání uložení nekonzistentních konfiguračních údajů. Co není možno zkontrolovat při uložení (komplexní vazení informace), je dodatečně kontrolováno a graficky zvýrazněno.
12.5	Řízení software	Řešení musí mít mechanismy pro detekci a zabránění instalaci nebo provádění škodlivého kódu (viry, trojské koně, červy ,.)	Plně splňuje	ve spolupráci s instalovaným antivirovým řešením
12.6	Řízení software	Aktualizace softwaru nesmí mít žádný vliv na uživatelskou komunikaci. K tomu musí mít systém různé komunikační mechanismy pro uživatele, administraci a maintenance. Pro každou aktualizaci softwaru musí být připravený mechanismus pro vrácení do stavu před aktualizací.	Plně splňuje	Nové verze aplikací jsou instalovány s možností návratu k původní verzi.
13	**Validace a integrita dat**			
13.1	Validace a integrita dat	V případě použití webového grafického rozhraní musí být vstupy dat (uživatelské i automatizované) ověřeny z pohledu správnosti (má-li být na vstupu číslo, nelze akceptovat písmeno) a integrity, je-li to technicky realizovatelné.	Plně splňuje	pro ověření vstupních hodnot je využívána sanitizace
13.2	Validace a integrita dat	V případě používání SW utilit, které mohou měnit stav/běh operačního systému či aplikace, musí být přístup k těmto nástrojům omezen a řízen.	Plně splňuje	závislé na implementaci a bezpečnostní politice zákazníka