MĚSTSKÁ ČÁST PRAHA 5

MĚSTSKÁ ČÁST PRAHA 5
ÚŘAD MĚSTSKÉ ČÁSTI PRAHA 5

Prohlášení o aplikovatelnosti – rozsah implementace

Říjen 2016

Nastavení souladu s požadavky dle normy ČSN ISO/IEC 27001:2014			Stav implementace	Odpovídá	Kontakty/Důkazy
A.5	**Politika bezpečnosti informací**				
A5.1	**Směřování bezpečnosti informací vedením organizace**				
Cíl:	Určit směr a vyjádřit podporu bezpečnosti informací ze strany vedení v souladu s požadavky týkající se činnosti organizace, příslušnými zákony a směrnicmi.			tajemník ÚMČ gestor správy bezpečnosti	
A.5.1.1	Politiky pro bezpečnost informací	Opatření: Soubor politik pro bezpečnost informací musí být definován, schválen vedením organizace, vydán a dán na vědomí všem zaměstnancům a relevantním externím stranám.		manažer bezpečnosti oblasti	Bc. Tesařová OKI
A.5.1.2	Přezkoumání politik pro bezpečnost informací	Opatření: Pro zajištění neustálé vhodnosti, přiměřenosti a efektivnosti musí být politiky pro bezpečnost informací přezkoumávány v plánovaných intervalech a vždy, když nastane významná změna.		interní auditor	Mgr. Ing. Poláčková
A.6	**Organizace bezpečnosti informací**				
A.6.1	**Interní organizace**				
Cíl:	Ustavit rámec řízení pro zahájení a řízení implementace a provozování bezpečnosti informací v organizaci.			tajemník ÚMČ gestor správy bezpečnosti	
A.6.1.1	Role a odpovědnosti bezpečnosti informací	Opatření: Musí být definovány a přiděleny odpovědnosti v oblasti bezpečnosti informací.		manažer bezpečnosti oblasti	Bc. Tesařová OKI
A.6.1.2	Princip oddělení povinností	Opatření: Pro snížení příležitostí k neoprávněné nebo neúmyslné modifikaci nebo zneužití aktiv organizace musí být zajištěno oddělení neslučitelných povinností a odpovědností.		manažer bezpečnosti oblasti	Bc. Tesařová OKI
A.6.1.3	Kontakt s příslušnými orgány a autoritami	Opatření: Musí být udržovány přiměřené vztahy s příslušnými orgány a autoritami.		manažer bezpečnosti oblasti	Bc. Tesařová OKI
A.6.1.4	Kontakt se zájmovými skupinami	Opatření: Musí být udržovány přiměřené vztahy s odbornými zájmovými skupinami nebo ostatními odbornými fóry na bezpečnost a profesními sdruženími.		manažer bezpečnosti oblasti	Bc. Tesařová OKI
A.6.1.5	Bezpečnost informací v řízení projektů	Opatření: Bezpečnost informací musí být zohledněna v řízení projektů nezávisle na typu projektu.		manažer bezpečnosti oblasti	Mgr. Viglaský OBK
A.6.2	**Mobilní zařízení a práce na dálku**				
Cíl:	Zajistit bezpečnost při použití mobilních zařízení a pro práci na dálku.				
A.6.2.1	Politika mobilních zařízení	Opatření: Musí být přijata politika a relevantní bezpečnostní opatření pro zvládání rizik spojených s používáním mobilních zařízení.		manažer bezpečnosti oblasti	Bc. Tesařová OKI

A.6.2.2	Práce na dálku	Opatření: Musí být implementována politika a relevantní opatření pro ochranu informací, které jsou přístupné, zpracovávané nebo ukládané v místech pro práci na dálku.		manažer bezpečnosti oblasti	Bc. Tesařová OKI
A.7	**Bezpčnost lidských zdrojů**				
A.7.1	**Před vznikem pracovního poměru**				
Cíl:	Zajistit, aby zaměstnaci a smluvní strany byli srozuměni se svými povinnostmi a aby pro jednotlivé role byli vybráni vhodní kandidáti.			tajemník ÚMČ gestor správy bezpečnosti	
A.7.1.1	Prověřování	Opatření: Všichni uchazeči o zaměstnání musí být prověřeni podle platných zákonů, předpisů a v souladu s etikou. Prověření musí být prováděna na základě požadavků týkajících se činností organizace, dále s ohledem na klasifikaci informací, ke kterým by měli získat přístup, a také z hlediska potencionálních rizik.		manažer bezpečnosti oblasti	Bc. Ďurišová
A.7.1.2	Podmínky pracovního vztahu	Opatření: Pracovní smlouvy uzavřené se zaměstnanci a smluvními stranami musí obsahovat ustanovení o jejich odpovědnostech a odpovědnostech organizace za bezpečnost informací.		manažer bezpečnosti oblasti	Bc. Ďurišová
A.7.2	**Bezpčnost lidských zdrojů**				
Cíl:	Zajistit, aby se zaměstnanci a smluvní strany byli vědomí a plnili si svoje povinnosti v oblasti bezpečnosti informací.			manažer bezpečnosti oblasti	Bc. Ďurišová, Bc. Tesařová
A.7.2.1	Odpovědnosti vedení organizace	Opatření: Vedení organizace musí po všech zaměstnancích a smluvních stranách požadovat dodržování bezpečnosti informací v souladu s ustavenými politikami.		manažer bezpečnosti oblasti	Bc. Ďurišová, Bc. Tesařová
A.7.2.2	Povědomí, vzdělávání a školení bezpečnosti informací	Opatření: Všichni zaměstnanci organizace, a je-li to relevantní i smluvní strany, musí s ohledem na svou pracovní náplň dostávat odpovídající vzdělávání a školení pro zvyšování povědomí bezpečnosti informací a musí být pravidelně informování o změnách v politikách a postupech bezpečnosti informací.		manažer bezpečnosti oblasti	Bc. Ďurišová, Bc. Tesařová
A.7.2.3	Disciplinární řízení	Opatření: Musí existovat formální proces disciplinárního řízení k přijetí opatření vůči zaměstnancům, kteří se dopustili narušení bezpečnosti informací.		tajemník ÚMČ gestor správy bezpečnosti	
A.7.3	**Ukončení a změna pracovního vztahu**				
Cíl:	Chránit zájmy organizace v rámci procesu změny nebo ukončení pracovního vztahu.				
A.7.3.1	Odpovědnost při ukončení nebo změně pracovního vztahu	Opatření: Odpovědnosti a povinnosti v oblasti bezpečnosti informací, které zůstávají platné po ukončení nebo změně pracovního vztahu, musí být definovány, komunikovány se zaměstnanci nebo smluvními stranami a prosazovány.		manažer bezpečnosti oblasti	Bc. Ďurišová
A.8	**Řízení aktiv**				
A.8.1	**Odpovědnost za aktiva**				

Cíl:	Identifikovat aktiva organizace a definovat odpovědnosti k jejich přiměřené ochraně.			tajemník ÚMČ gestor správy bezpečnosti	
A.8.1.1	Seznam aktiv	Opatření: Aktiva související s informacemi a vybavení pro zpracování informací musí být identifikována a seznam těchto aktiv musí být vytvořen a udržován.		manažer bezpečnosti oblasti	Mgr. Viglaský, Bc. Tesařová
A.8.1.2	Vlastnictví aktiv	Opatření: Aktiva udržována v seznamu musí mít určeného vlastníka.		manažer bezpečnosti oblasti	Mgr. Viglaský, Bc. Tesařová
A.8.1.3	Přípustné použití aktiv	Opatření: Musí být určena, dokumentována a implementována pravidla pro přípustné použití informací a aktiv souvisejících s informacemi a vybavením pro zpracování informací.		manažer bezpečnosti oblasti	Bc. Tesařová OKI
A.8.1.4	Navrácení aktiv	Opatření: Při ukončení pracovního vztahu, smluvního vztahu nebo dohody musí zaměstnanci a pracovníci externích stran odevzdat veškerá jim svěřená aktiva, která jsou majetkem organizace.		manažer bezpečnosti oblasti	Bc.Tesařová, Bc. Ďurišová, Mgr. Viglaský
A.8.2	**Klasifikace informací**				
Cíl:	Zajistit, aby informamce získaly odpovídající úroveň ochrany v souladu s jejich důležitostí pro organizaci.			tajemník ÚMČ gestor správy bezpečnosti	
A.8.2.1	Klasifikace informací	Opatření: Informace musí být klasifikovány s ohledem na zákonné požadavky, jejich hodnotu, kritičnost a citlivost vůči neoprávněnému prozrazení nebo modifikací.		manažer bezpečnosti oblasti	Mgr. Klein, Mgr. Viglaský, Bc. Tesařová
A.8.2.2	Označování informací	Opatření: Pro označování informací musí být vytvořen a implementován vhodný soubor postupů, které jsou v souladu se schématem klasifikace informací přijatým organizací.		manažer bezpečnosti oblasti	Mgr. Viglaský, Bc. Tesařová
A.8.2.3	Manipulace s aktivy	Opatření: Pro manipulaci s aktivy musí být vytvořeny a implementovány postupy v souladu se schématem klasifikace informací přijatým organizací.		manažer bezpečnosti oblasti	Mgr. Viglaský, Bc. Tesařová
A.8.3	**Manipulace s médii**				
Cíl:	Předcházet neoprávněnému vyzrazení, modifikací, odstranění nebo zničení informací uložených na médiích.			manažer bezpečnosti oblasti	
A.8.3.1	Správná výměna médií	Opatření: Musí být implementovány postupy pro správu výměnných médií v souladu se schématem klasifikace infromací přijatým organizací.		manažer bezpečnosti oblasti	Bc. Tesařová OKI
A.8.3.2	Likvidace médií	Opatření: Média, pokud nejsou dále upotřebitelná, musí být bezpečně zlikvidována v souladu s formalizovanými postupy.		manažer bezpečnosti oblasti	Bc. Tesařová OKI
A.8.3.3	Přeprava fyzických médií	Opatření: Média obsahujícíc informace musí být během přepravy chráněna proti neoprávněnému přístupu, zneužití nebo narušení.		manažer bezpečnosti oblasti	Bc. Tesařová OKI
A.9	**Řízení přístupu**				
A.9.1	**Požadavky organizace na řízení přístupu**				

Cíl:	Omezit přístup k informacím a vybavení pro zpracování informací.			tajemník ÚMČ gestor správy bezpečnosti	Bc. Tesařová OKI
A.9.1.1	Politika řízení přístupu	Opatření: Musí být ustavena, dokumentována a přezkoumávána politika řízení přístupu v závislosti na požadavcích na činnosti organizace a bezpečnosti informací.		manažer bezpečnosti oblasti	Mgr. Viglaský, Bc. Tesařová
A.9.1.2	Přístup k sítím a síťovým službám	Opatření: Uživatelé musí mít přístup pouze k těm sítím a síťovým službám, pro jejichž použití byli zvlášť oprávněni.		manažer bezpečnosti oblasti	Bc. Tesařová OKI
A.9.2	**Řízení přístupů uživatelů**				
Cíl:	Zajistit oprávněný přístup uživatelů a předcházet neoprávněnému přístupu k systémům a službám.			manažer bezpečnosti oblasti	
A.9.2.1	Registrace a zrušení registrace uživatele	Opatření: Pro přidělování přístupových práv musí být implementován proces formalizované registrace uživatele včetně jejího zrušení.		manažer bezpečnosti oblasti	Mgr. Viglaský, Bc. Tesařová
A.9.2.2	Správa uživatelských přístupů	Opatření: Pro přidělování a odebírání přístupových práv všem typům uživatelů ke všem systémům a službám musí být implementován formalizovaný proces správy uživatelských přístupů.		manažer bezpečnosti oblasti	Bc. Tesařová OKI
A.9.2.3	Správa privilegovaných přístupových práv	Opatření: Musí být omezeno a řízeno přidělování a používání privilegovaných práv.		manažer bezpečnosti oblasti	Bc. Tesařová OKI
A.9.2.4	Správa tajných autentizačných informací uživatelů	Opatření: Přidělování tajných autentizačních informací musí být řízeno formalizovaným procesem.		NEREALIZOVANÉ	
A.9.2.5	Přezkoumání přístupových práv uživatelů	Opatření: Vlastníci aktiv musí v pravidelných intervalech přezkoumávat přístupová práva uživatelů.		manažer bezpečnosti oblasti	Bc. Tesařová OKI
A.9.2.6	Odebírání nebo úprava přístupových práv	Opatření: Při ukončení nebo změně pracovního vstahu, smluvního vstahu nebo dohody musí být všem zaměstnancům a externím stranám odejmuta nebo pozměněna přístupová práva k informacím a vybavení pro zpracování informací.		manažer bezpečnosti oblasti	Bc.Tesařová, Bc. Ďurišová, Mgr. Viglaský
A.9.3	**Odpovědnost uživatelů**				
Cíl:	Učinit uživatele odpovědné za ochranu jejich autentizačních informací.			manažer bezpečnosti oblasti	
A.9.3.1	Používání tajných autentizačních informací	Opatření: Při používání tajných autentizačních informací musí být po uživatelích vyžadováno, aby dodržovali postupy stanovené organizací.		NEREALIZOVANÉ	
A.9.4	**Řízení přístupu k systémům a aplikacím**				
Cíl:	Předcházet neautorizovanému přístupu k systémům a aplikacím.			manažer bezpečnosti oblasti	
A.9.4.1	Omezení přístupu k informacím	Opatření: V souladu s politikou řízení přístupu musí být omezen přístup k informacím a funkcím aplikací.		manažer bezpečnosti oblasti	Bc. Tesařová OKI

A.9.4.2	Bezpečné postupy přihlášení	Opatření: Pokud to politika řízení přístupu vyžaduje, musí být přístup k systémům a aplikacím řízen postupy bezpečného přihlášení.		manažer bezpečnosti oblasti	Bc. Tesařová OKI
A.9.4.3	Systém správy hesel	Opatření: Systém správy hesel musí být interaktivní a musí zajišťovat použití kvalitních hesel.		manažer bezpečnosti oblasti	Bc. Tesařová OKI
A.9.4.4	Použití privilegovaných programových nástrojů	Opatření: Musí být omezeno a přísně kontrolováno použití programových nástrojů, které mohou být schopné překonat systémové nebo aplikační kontroly.		manažer bezpečnosti oblasti	Bc. Tesařová OKI
A.9.4.5	Řízení přístupu ke zdrojovým kódům programů	Opatření: Musí být omezen přístup ke zdrojovým kódům programů.		manažer bezpečnosti oblasti	Bc. Tesařová OKI
A.10	**Kryptografie**				
A.10.1	**Kryptografická opatření**				
Cíl:	Zajistit řádné a efektivní používání kryptografie k ochraně důvěrnosti, autentičnosti a/nebo integrity informací.			NEREALIZOVANÉ	
A.10.1.1	Politika použití kryptografických opatření	Opatření: Musí být vytvořena a implementována politika pro používání kryptografických opatření na ochranu informací.		NEREALIZOVANÉ	
A.10.1.2	Správa klíčů	Opatření: Politika pro používání, ochranu a dobu existence kryptografických klíčů musí být vytvořena a implementována po celou dobu jejich životního cyklu.		NEREALIZOVANÉ	
A.11	**Fyzická bezpečnost a bezpečnost prostředí**				
A.11.1	**Bezpečné oblasti**				
Cíl:	Předcházet neautorizovanému fyzickému přístupu, poškození a zásahům do informací a vybavení pro zpracování infromací organizace.			tajemník ÚMČ gestor správy bezpečnosti	
A.11.1.1	Fyzický bezpečnostní perimetr	Opatření: Bezpečnostní perimetry musí být definovány a používány k ochraně oblastí, které obsahují citlivé nebo kritické informace a vybavení pro zpracování informací.		manažer bezpečnosti oblasti	Šimko OBK
A.11.1.2	Fyzické kontroly vstupu	Opatření: Aby bylo zajištěno, že je přístup do bezpečných oblastí povolen pouze oprávněným osobám, musí být tyto oblasti chráněny vhodným systémem vstupních kontrol.		manažer bezpečnosti oblasti	Šimko OBK,
A.11.1.3	Zabezpečení kanceláří, místností a vybavení	Opatření: Musí být navržena a aplikována fyzická bezpečnost kanceláří, místností a vybavení.		manažer bezpečnosti oblasti	Šimko OBK,
A.11.1.4	Ochrana před vnějšími hrozbami a hrozbami prostředí	Opatření: Musí být navržena a aplikována fyzická ochrana proti přírodním katastrofám, úmyslému útoku a haváriím.		manažer bezpečnosti oblasti	Šimko OBK,
A.11.1.5	Práce v bezpečných oblastch	Opatření: Musí být navrženy a aplikovány postupy pro práci v zabezpečených oblastech.		manažer bezpečnosti oblasti	Šimko OBK,

A.11.1.6	Oblasti pro nakládku a vykládku	Opatření: Přístupové body, jako oblasti pro nakládku a vykládku a další místa, kde se mohou neoprávněné osoby dostat do prostor organizace, musí být kontrolovány, a pokud je to možné, izolovány od vybavení pro zpracování informací, aby se zabránilo neoprávněnému přístupu k nim.		manažer bezpečnosti oblasti	Šimko OBK,
A.12	**Bezpečnost provozu**				
A.12.1	**Provozní postupy a odpovědnosti**				
Cíl:	Zabezpečit správný a bezpečný provoz vybavení pro zpracování informací.			tajemník ÚMČ gestor správy bezpečnosti	
A.12.1.1	Dokumentované provozní postupy	Opatření: Provozní postupy musí být dokumentovány a musí být dostupné všem uživatelům podle potřeby.		manažer bezpečnosti oblasti	Mgr. Viglaský OBK
A.12.1.2	Řízení změn	Opatření: Změny v organizaci a jejich procesech, v prostředcích pro zpracovávání informací a systémech, které ovlivňují bezpečnost informací, musí být řízeny.		manažer bezpečnosti oblasti	Bc.Tesařová, Bc. Ďurišová, Mgr. Viglaský
A.12.1.3	Řízení kapacit	Opatření: Pro zajištění požadovaného výkonu systému, s ohledem na budoucí kapacitní požadavky, musí být monitorováno, nastaveno a předvídáno využití zdrojů.		manažer bezpečnosti oblasti	Mgr. Viglaský, Bc. Tesařová
A.12.1.4	Princip oddělení prostředí vývoje, testování a provozu	Opatření: Pro snížení rizika neoprávněného přístupu nebo změn provozního prostředí musí být odděleno prostředí vývoje, testování a provozu.		manažer bezpečnosti oblasti	Mgr. Viglaský, Bc. Tesařová
A.12.2	**Ochrana proti malware**				
Cíl:	Zajistit, aby informace a vybavení pro zpracování informací byly chráněny proti malware.			manažer bezpečnosti oblasti	
A.12.2.1	Opatření proti malware	Opatření: Na ochranu proti malware musí být implementována opatření na jejich detekci, prevenci a obnovu, a to ve spojení s odpovídajícím bezpečnostním povědomím uživatelů.		manažer bezpečnosti oblasti	Bc. Tesařová OKI
A.12.3	**Zálohování**				
Cíl:	Chránit proti ztrátě dat.			manažer bezpečnosti oblasti	
A.12.3.1	Zálohování informací	Opatření: Záložní kopie informací, software a binárních obrazů systému musí být pořizovány a testovány v pravidelných intervalech v souladu se schválenou politikou zálohování.		manažer bezpečnosti oblasti	Bc. Tesařová OKI
A.12.4	**Zaznamenávání formou logů a monitoring**				
Cíl:	Zaznamenávat události a vytvářet záznamy.			manažer bezpečnosti oblasti	
A.12.4.1	Zaznamenávání událostí formou logů	Opatření: Musí být pořizovány, uchovány a pravidelně přezkoumávány logy události zaznamenávající aktivity uživatelů, výjimky, selhání a události bezpečnosti informací.		manažer bezpečnosti oblasti	Bc. Tesařová OKI
A.12.4.2	Ochrana logů	Opatření: Prostředky pro zaznamenávání formou logů a logy musí být chráněny proti zfalšování a neoprávněnému přístupu.		manažer bezpečnosti oblasti	Bc. Tesařová OKI

A.12.4.3	Logy o činnosti administrátorů a operátorů	Opatření: Aktivity systémového administrátora a systémového operátora musí být logovány a logy chráněny a pravidelně přezkoumávány.		manažer bezpečnosti oblasti	Bc. Tesařová OKI
A.12.4.4	Synchronizace hodin	Opatření: Hodiny všech důležitých systémů pro zpracování informací musí být v rámci organizace nebo bezpečnostních domén synchronizovány s jediným referenčním zdrojem času.		manažer bezpečnosti oblasti	Bc. Tesařová OKI
A.12.5	**Správa provozního software**				
Cíl:	Zajistiti integritu provozních systémů			manažer bezpečnosti oblasti	
A.12.5.1	Instalace software na provozní systémy	Opatření: Musí být implementovány postupy řízené instalace softwaru na provozních systémech.		manažer bezpečnosti oblasti	Bc. Tesařová OKI
A.12.6	**Řízení technických zranitelností**				
Cíl:	Zabránit využívání technických zranitelností.			manažer bezpečnosti oblasti	
A.12.6.1	Řízení technických zranitelností	Opatření: Musí být zajištěno včasné získání informací o existenci technických zranitelností provozovaných informačních systémů, vyhodnocena úroveň ohrožení organizace vůči těmto zranitelnostem a přijata příslušná opatření na zvládání souvisejících rizik.		manažer bezpečnosti oblasti	Bc. Tesařová OKI
A.12.6.2	Omezení instalace software	Opatření: Musí být ustavena a implementována pravidla ohledně instalace software uživateli.		manažer bezpečnosti oblasti	Bc. Tesařová OKI
A.12.7	**Hlediska auditu informačních systémů**				
Cíl:	Minimalizovat dopady auditních činností na provozní systémy.			manažer bezpečnosti oblasti	
A.12.7.1	Opatření k auditu infromačních systémů	Opatření: Požadavky auditu a činnosti zahrnující verifikaci provozních systémů musí být pečlivě naplánovány a schváleny, aby se minimalizovalo narušení procesů organizace.		manažer bezpečnosti oblasti	Bc. Tesařová OKI
A.13	**Bezpečnost komunikací**				
A.13.1	**Správa bezpečnosti sítě**				
Cíl:	Zajistit ochranu informací v sítích a jejich podpůrných prostředcích pro zpracování informací.			tajemník ÚMČ gestor správy bezpečnosti	
A.13.1.1	Opatření v sítích	Opatření: K ochraně informací v systémech a aplikacích musí být sítě řízeny, spravovány a kontrolovány.		manažer bezpečnosti oblasti	Bc. Tesařová OKI
A.13.1.2	Bezpečnost síťových služeb	Opatření: Musí být identifikovány a do dohod o poskytování síťových služeb zahrnuty bezpečnostní mechanismy, úroveň poskytovaných služeb a požadavky na správu všech síťových služeb, ať už jsou zajišťovány interně nebo cestou outsourcingu.		manažer bezpečnosti oblasti	Bc. Tesařová OKI
A.13.1.3	Princip oddělení v sítích	Opatření: V sítích musí být oddělenz skupiny informačních služeb, uživatelů a informačních systémů.		manažer bezpečnosti oblasti	Bc. Tesařová OKI
A.13.2	**Přenos informací**				

Cíl:	Zajistit bezpečnost informací při jejich přenosu v rámci organizace a s externími subjekty.			manažer bezpečnosti oblasti	
A.13.2.1	Politiky a postupy při přenosu informací	Opatření: Musí existovat formalizované politiky, postupy a opatření k ochraně přenosu infromací pomocí jakéhokmoliv tzpu komunikačního vybavení.		manažer bezpečnosti oblasti	Bc. Tesařová OKI
A.13.2.2	Dohody o přenosu informací	Opatření: Dohody se musí zabývat zabezpečeným přenosem infromací týkající se činnosti orgnaizace mezi organizací a externími stranami.		manažer bezpečnosti oblasti	Bc. Tesařová OKI
A.13.2.3	Elektronické předávání zpráv	Opatření: Musí být vhodným způsobem chráněny elektronicky přenášené informace.		manažer bezpečnosti oblasti	Bc. Tesařová OKI
A.13.2.4	Dohody o utajení nebo o mlčenlivosti	Opatření: Musí být identifikovány, pravidelně přezkoumávány a dokumentovány požadavky na dohody o utajení nebo na dohody o mlčenlivosti reflektující potřeby organizace na ochranu informací.		manažer bezpečnosti oblasti	Bc. Tesařová OKI
A.14	**Akvizice, vývoj a údržba systémů**				
A.14.1	**Bezpečnostní požadavky infromačních systémů**				
Cíl:	Zajistit, aby se bezpečnost infromací stala nedílnou součástí infromačních systémů v jejich celém životním cyklu. To zahrnuje i požadavky na informační systémy, které poskytují služby ve veřejných sítích.			tajemník ÚMČ gestor správy bezpečnosti	
A.14.1.1	Analýza a specifikace požadavků bezpečnosti informací	Opatření: V požadavcích na nové informační systémy nebo na rozšíření existujících systémů musí být obsaženy také požadavky týkající se bezpečnosti informací.		manažer bezpečnosti oblasti	Bc. Tesařová OKI
A.14.1.2	Zabezpečení aplikačních služeb ve veřejných sítích	Opatření: Infromace přenášené ve veřejných sítích v rámci aplikačních služeb musí být chráněny před podvodnými aktivitami, zpochybňováním smluv, neoprávněným vyzrazením a modifikací.		manažer bezpečnosti oblasti	Bc. Tesařová OKI
A.14.1.3	Ochrana transakcí aplikačních služeb	Opatření: Musí být zajištěna ochrana infromací přenášených při transakcích aplikačních služeb tak, aby se zabránilo neúplnému přenosu informací, chybnému směřování, neoprávněné změně zpráv, neoprávněnému vyzrazení, neoprávněné duplikaci nebo opakování přenosu zpráv.		manažer bezpečnosti oblasti	Bc. Tesařová OKI
A.14.2	**Bezpečnost v procesech vývoje a podpory**				
Cíl:	Zajistit, aby bezpečnost informací byla navrhována a implementována v životním cyklu vývoje informačních systémů.			manažer bezpečnosti oblasti	
A.14.2.1	Politika bezpečného vývoje	Opatření: Musí být ustavena a v rámci organizace aplikována pravidla pro vývoj softwaru a systémů.		manažer bezpečnosti oblasti	Bc. Tesařová OKI
A.14.2.2	Postupy řízení změn systémů	Opatření: Pomocí formalizovaných postupů řízení změn musí být řízeny změny systémů v rámci jejich životního cyklu vývoje.		manažer bezpečnosti oblasti	Bc. Tesařová OKI

A.14.2.3	Technická přezkoumání aplikací po změnách provozní platformy	Opatření: V případě změny provozní platformy musí být přezkoumány a otestovány aplikace kritické pro činnost organizace, aby se zajistilo, že změny nemají nepříznivý dopad na provoz nebo bezpečnost organizace.		manažer bezpečnosti oblasti	Bc. Tesařová OKI
A.14.2.4	Omezení změn softwarových balíků	Opatření: Modifikace softwarových balíků musí být omezeny na nezbytné změny a veškeré prováděné změny musí být přísně řízeny.		manažer bezpečnosti oblasti	Bc. Tesařová OKI
A.14.2.5	Principy budování bezpečných systémů	Opatření: Principy budování bezpečných systémů musí být ustaveny, dokumentovány, udržovány a aplikovány při implementaci informačních systémů.		manažer bezpečnosti oblasti	Bc. Tesařová OKI
A.14.2.6	Prostředí bezpečného vývoje	Opatření: Pro vývoj systémů a jejich integrací, překrývající celý životní cyklus vývoje systémů, musí organizace vytvořit a přiměřeně chránit prostředí bezpečného vývoje systému.		manažer bezpečnosti oblasti	Bc. Tesařová OKI
A.14.2.7	Outsourcovaný vývoj	Opatření: Organizace musí dohlížet a monitorovat činnosti outsourcovaného vývoje systému.		manažer bezpečnosti oblasti	Bc. Tesařová OKI
A.14.2.8	Testování bezpečnosti systému	Opatření: Během vývoje musí být prováděno testování funkčnosti bezpečnosti.		manažer bezpečnosti oblasti	Bc. Tesařová OKI
A.14.2.9	Testování akceptace systému	Opatření: Pro nové informační systémy, aktualizace a nové verze musí být ustaveny testovací postupy a odpovídající kriteria akceptace.		manažer bezpečnosti oblasti	Bc. Tesařová OKI
A.14.3	**Data pro testování**				
Cíl:	Zajistit ochranu dat používaných pro testování.			manažer bezpečnosti oblasti	
A.14.3.1	Ochrana dat pro testování	Opatření: Data pro testování musí být pečlivě vybrána, chráněna a kontrolována.		manažer bezpečnosti oblasti	Bc. Tesařová OKI
A.15	**Dodavatelské vztahy**				
A.15.1	**Bezpečnost infromací v dodavatelských vztazích**				
Cíl:	Zajistit ochranu aktiv organizace, ke kterým mají dodavtelé přístup			tajemník ÚMČ gestor správy bezpečnosti	
A.15.1.1	Politika bezpečnosti informací pro dodavatelské vztahy	Opatření: Požadavky bezpečnosti informací na snížení rizik spojených s přístupem dodavatelů k aktivům organizace musí být odsouhlasený s dodavateli a dokumentovány.		manažer bezpečnosti oblasti	Bc. Tesařová OKI
A.15.1.2	Bezpečnostní požadavky v dohodách a dodavateli	Opatření: Všechny požadavky relevantní bezpečnosti informací musí být ustaveny a odsouhlaseny s každým dodavatelem, který může přistupovat k infromacím organizace, zpracovávat je, ukládat, komunikovat nebo je zajišťovat prvky IT infrastruktury.		manažer bezpečnosti oblasti	Bc. Tesařová OKI

A.15.1.3	Dodavatelský řetězec informačních a komunikačních technologií	Opatření: Dohoda s dodavateli musí zahrnovat požadavky na rizika bezpečnosti informací spojená s dodavatelským řetězcem služeb a produktů informačních a komunikačních technologií.		manažer bezpečnosti oblasti	Bc. Tesařová OKI
A.15.2	**Řízení dodávek služeb dodavatelů**				
Cíl:	Udržovat dohodnutou úroveň bezpečnosti informací a dodávky služeb ve shodě s dodavatelskými dohodami.			manažer bezpečnosti oblasti	
A.15.2.1	Monitorování a přezkoumávání služeb dodavatelů	Opatření: Organizace musí pravidelně monitorovat, přezkoumávat a auditovat dodávky služeb dodavatelů.		manažer bezpečnosti oblasti	Bc. Tesařová OKI
A.15.2.2	Řízení změn ve službách dodavatelů	Opatření: Změny v poskytování služeb dodavateli, včetně změn v udržování a zlepšování existujících politik, postupů a opatření bezpečnosti informací, musí být řízeny s ohledem na kritičnost informací, systémů a procesů organizace, které jsou součásti těchto změn, a s ohledem na opakované posouzení rizik.		manažer bezpečnosti oblasti	Bc. Tesařová OKI
A.16	**Řízení incidentů bezpečnosti informací**				
A.16.1	**Řízení incidentů bezpečnosti informací a zlepšování**				
Cíl:	Zajistit odpovídající a efektivní přístup ke zvládání incidentů bezpečnosti informací zahrnujícímu komunikaci ohledně bezpečnostních událostí a slabých míst.			tajemník ÚMČ gestor správy bezpečnosti	
A.16.1.1	Odpovědnosti a postupy	Opatření: Pro zajištění rychlé, efektivní a systematické reakce na incidenty bezpečnosti informací musí být ustaveny odpovědnosti a postupy pro zvládání incidentů bezpečnosti informací.		manažer bezpečnosti oblasti	Bc. Tesařová OKI
A.16.1.2	Hlášení událostí bezpečnosti informací	Opatření: Události bezpečnosti informací musí být co nejrychleji hlášeny příslušnými řídícími kanály.		manažer bezpečnosti oblasti	Bc. Tesařová OKI, Šimko OBK
A.16.1.3	Hlášení slabých míst bezpečnosti informací	Opatření: Po zaměstnancích a smluvních stranách používají informační systémy a služby musí být vyžadováno, aby si všímali a hlásili jakákoliv slabá místa bezpečnosti informací v systémech nebo službách nebo podezření na ně.		manažer bezpečnosti oblasti	Bc. Tesařová OKI
A.16.1.4	Posouzení a rozhodnutí o událostech bezpečnosti informací	Opatření: Události bezpečnosti informací musí být posouzeny a musí být rozhodnuto, zd mají být klasifikovány jako incidenty bezpečnosti informací.		manažer bezpečnosti oblasti	Bc. Tesařová OKI, Šimko OBK
A.16.1.5	Reakce na incidenty bezpečnosti informací	Opatření: Reakce na incidentybezpečnosti informací musí být v souladu s dokumentovanými postupy.		manažer bezpečnosti oblasti	Bc. Tesařová OKI
A.16.1.6	Ponaučení z incidentů bezpečnosti informací	Opatření: Znalosti získané z analýzy a řešení incidentů bezpečnosti informací musí být použity ke snížení pravděpodobnosti nebo dopadu následných incidentů.		manažer bezpečnosti oblasti	Bc. Tesařová OKI, Šimko OBK
A.16.1.7	Shromažďování důkazů	Opatření: Organizace musí definovat a aplikovat postupy pro identifikaci, sběr získání a uchování informací, které můžou sloužit jako důkazy.		manažer bezpečnosti oblasti	Bc. Tesařová OKI
A.17	**Aspekty řízení kontinuity činností organizace z hlediska bezpečnosti informací**				

A.17.1	**Kontinuita bezpečnosti infromací**				
Cíl:	Kontinuita bezpečnosti informací musí být součásti systémů řízení kontinuity činností organizace.			tajemník ÚMČ gestor správy bezpečnosti	
A.17.1.1	Plánování kontinuity bezpečnosti informací	Opatření: Organizace musí určit svoje požadavky na bezpečnost informací a kontinuitu řízení bezpečnosti informací při nepříznivých situacích, například během krizí, katastrof nebo havárií.		manažer bezpečnosti oblasti	Bc. Tesařová OKI
A.17.1.2	Implementace kontinuity bezpečnosti informací	Opatření: Organizace musí ustavit, dokumentovat, implementovat a udržovat procesy, postupy a opatření k zajištění požadované úrovně kontinuity pro bezpečnost informací během nepříznivých situací.		manažer bezpečnosti oblasti	Bc. Tesařová OKI
A.17.1.3	Verifikace, přezkoumání a vyhodnocení kontinuity bezpečnosti informací	Opatření: Organizace musí v pravidelných intervalech verifikovat ustavená a implementovaná opatření kontinuity bezpečnosti informací, aby zajistila, že jsou dostatečná a efektivní během nepříznivých situací.		manažer bezpečnosti oblasti	Bc. Tesařová OKI
A.17.2	**Redundance**				
Cíl:	Zajistit dostupnost vybavení pro zpracování informací.			manažer bezpečnosti oblasti	
A.17.2.1	Dostupnost vybavení pro zpracování informací	Opatření: Vybavení pro zpracování informací musí být integrováno s dostatečnou redundancí, aby byly splněny požadavky na dostupnost.		manažer bezpečnosti oblasti	Bc. Tesařová OKI
A.18	**Soulad s požadavky**				
A.18.1	**Soulad s právními a smluvními požadavky**			tajemník ÚMČ gestor správy bezpečnosti	
Cíl:	Vyvarovat se porušení zákonných, předpisových nebo smluvních povinností týkající se bezpečnosti informací a jakýchkoliv bezpečnostních požadavků.			manažer bezpečnosti oblasti	
A.18.1.1	Identifikace odpovídající legislativy a smluvních požadavků	Opatření: Pro každý informační systém a organizaci musí být jednoznačně identifikovány, dokumentovány a udržovány aktuální veškeré relevantní zákonné, předpisové a smluvní požadavky a způsob, jakým je organizace dodržuje.		manažer bezpečnosti oblasti	Mgr. Klein, Mgr. Viglaský, Bc. Tesařová
A.18.1.2	Ochrana duševního vlastnictví	Opatření: Pro zajištění souladu se zákonnými, předpisovými a smluvními požadavky, které jsou relevantní ochraně duševního vlastnictví a používáníproprietárních softwarových produktů, musí být implementovány vhodné postupy.		manažer bezpečnosti oblasti	Mgr. Klein, Mgr. Viglaský, Bc. Tesařová
A.18.1.3	Ochrana záznamů	Opatření: Záznamy musí být chráněny proti ztrátě, zničení, padělání a neautorizovanému přístupu a zveřejnění, a to v souladu se zákonnými, předpisovými a smluvními požadavky a požadavky týkající se činností organizace.		manažer bezpečnosti oblasti	Mgr. Klein, Mgr. Viglaský, Bc. Tesařová
A.18.1.4	Soukromí a ochrana osobních údajů	Opatření: Soukromí a ochrana osobních údajů musí být zajištěny v souladu s odpovídající legislativou a předpisy, pokud je to použitelné.		manažer bezpečnosti oblasti	Mgr. Klein, Mgr. Viglaský, Bc. Tesařová, Šimko
A.18.1.5	Regulace kryptografických opatření	Opatření: Kryptografická opatření musí být používána v souladu s příslušnými úmluvami, legislativou a předpisy.		NEREALIZOVANÉ	
A.18.2	**Přezkoumání bezpečnosti infromací**				

Cíl:	Zajistit, že bezpečnost informací je implementována v souladu s politikami a postupy organizace.			manažer bezpečnosti oblasti	
A.18.2.1	Nezávislá přezkoumání bezpečnosti informací	Opatření: Přístup organizace k řízení a implementaci bezpečnosti informací (tj. cílů opatření, jednotlivých opatření, politik, procesů a postupů bezpečnosti informací) musíí být nezávisle přezkoumáván v plánovaných intervalech, nebo když nastane významná změna.		manažer bezpečnosti oblasti	Mgr. Viglaský, Bc. Tesařová
A.18.2.2	Shoda s bezpečnostními politikami a normami	Opatření: Vedoucí pracovníci musí pravidelně přezkoumávat shodu zpracování informací a postupů v rozsahu jejich odpovědností s odpovídajícími bezpečnostními politikami, normami a dalšími požadavky na bezpečnost.		manažer bezpečnosti oblasti	Mgr. Viglaský, Bc. Tesařová
A.18.2.3	Přezkoumání technické shody	Opatření: Informační systémy musí být pravidelně přezkoumávány, zda jsou v souladu s politikami a normamibezpečnosti informací organizace.		manažer bezpečnosti oblasti	Mgr. Viglaský, Bc. Tesařová

V Praze dne:

19 -10- 2016

Mgr. Pavel Radovan Viglaský, MPA
manažer bezpečnosti oblasti procesů

Bc. Josef Žebera
pověřen výkonem funkce tajemníka ÚMČ Praha 5
gestor správy bezpečnosti