ISMS_PoA

Prohlášení o aplikovatelnosti přílohy A ISO/IEC 27001:2013 CZ
Součást systému řízení informační bezpečnosti CS SOFT, a.s.

Ref příloha A	Název	Aplikováno?
	A.5 Politiky bezpečnosti informací	
A.5.1	**Směřování bezpečnosti informací vedením organizace**	
A.5.1.1	Politiky informační bezpečnosti	**Ano**
A.5.1.2	Přezkoumání politik bezpečnosti informací	**Ano**
	A.6 Ogranizace bezpečnosti informací	
A.6.1	**Interní organizace**	
A.6.1.1	Role a odpovědnosti k informační bezpečnosti	**Ano**
A.6.1.2	Oddělení povinností	**Ano**
A.6.1.3	Kontakt s orgány veřejné správy	**Ano**
A.6.1.4	Kontakt se zájmovými skupinami	**Ano**
A.6.1.5	Informační bezpečnost v projektovém řízení	**Ano**
A.6.2	**Mobilní zařízení a práce na dálku**	
A.6.2.1	Politika mobilních zařízení	**Ano**
A.6.2.2	Práce z domova	**Ano**
	A.7 Bezpečnost lidských zdrojů	
A.7.1	**Před vznikem pracovního vztahu**	
A.7.1.1	Prověřování	**Ano**
A.7.1.2	Podmínky pracovního vztahu	**Ano**
A.7.2	**Během pracovního poměru**	
A.7.2.1	Odpovědnosti vedení organizace	**Ano**
A.7.2.2	Povědomí, vzdělávání a školení bezpečnosti informací	**Ano**
A.7.2.3	Disciplinární řízení	**Ano**
A.7.3	**Ukončení a změna pracovního vztahu**	
A.7.3.1	Odpovědnosti při ukončení nebo změně pracovního vztahu	**Ano**
	A.8 Řízení aktiv	
A.8.1	**Odpovědnost za aktiva**	
A.8.1.1	Seznam aktiv	**Ano**
A.8.1.2	Vlastnictví aktiv	**Ano**
A.8.1.3	Přípustné použití aktiv	**Ano**
A.8.1.4	Navrácení aktiv	**Ano**
A.8.2	**Klasifikace informací**	
A.8.2.1	Klasifikace informací	**Ano**
A.8.2.2	Označování informací	**Ano**
A.8.2.3	Manipulace s aktivy	**Ano**
A.8.3	**Manipulace s médii**	
A.8.3.1	Správa přenosných médií	**Ano**
A.8.3.2	Likvidace médií	**Ano**
A.8.3.3	Přeprava fyzických médií	**Ano**
	A.9 Řízení přístupu	
A.9.1	**Požadavky organizace na řízení přístupu**	
A.9.1.1	Politika řízení přístupu	**Ano**
A.9.1.2	Přístup k sítím a síťovým službám	**Ano**
A.9.2	**Řízení přístupu uživatelů**	
A.9.2.1	Registrace a zrušení registrace uživatelů	**Ano**
A.9.2.2	Správa uživatelských přístupů	**Ano**
A.9.2.3	Správa privilegovaných přístupových práv	**Ano**
A.9.2.4	Správa tajných autentizačních informací uživatelů	**Ano**
A.9.2.5	Přezkoumání přístupových práv uživatelů	**Ano**
A.9.2.6	Odebrání nebo úprava přístupových práv	**Ano**
A.9.3	**Odpovědnosti uživatelů**	
A.9.3.1	Používání tajných autentizačních informací	**Ano**
A.9.4	**Řízení přístupu k systémům a informacím**	

A.9.4.1	Omezení přístupu k informacím	**Ano**
A.9.4.2	Bezpečené způsoby přihlášení	**Ano**
A.9.4.3	Systém správy hesel	**Ano**
A.9.4.4	Použití privilegovaných programových nástrojů	**Ano**
A.9.4.5	Řízení přístupu ke zdrojovým kódům programů	**Ano**
A.10 Kryptogtafie		
A.10.1	**Kryptografická opatření**	
A.10.1.1	Politika pro použití kryptografických opatření	**Ano**
A.10.1.2	Správa klíčů	**Ano**
A.11 Fyzická bezpečnost a bezpečnost prostředí		
A.11.1	**Bezpečné oblasti**	
A.11.1.1	Fyzický bezpečnostní perimetr	**Ano**
A.11.1.2	Fyzické kontroly vstupu	**Ano**
A.11.1.3	Zabezpečení kanceláří, místností a vybavení	**Ano**
A.11.1.4	Ochrana před vnějšími hrozbami a hrozbami prostředí	**Ano**
A.11.1.5	Práce v bezpečných oblastech	**Ano**
A.11.1.6	Oblasti pro nakládku a vykládku	**Ano**
A.11.2	**Zařízení**	
A.11.2.1	Umístění zařízení a jeho ochrana	**Ano**
A.11.2.2	Podpůrné služby	**Ano**
A.11.2.3	Bezpečnost kabelových rozvodů	**Ano**
A.11.2.4	Údržba zařízení	**Ano**
A.11.2.5	Přemístění aktiv	**Ano**
A.11.2.6	Bezpečnost zařízení a aktiv mimo prostory organizace	**Ano**
A.11.2.7	Bezpečná likvidace nebo opakované použití zařízení	**Ano**
A.11.2.8	Uživatelská zařízení bez obsluhy	**Ano**
A.11.2.9	Zásada prázdného stolu a prázdné obrazovky monitoru	**Ano**
A.12 Bezpečnost provozu		
A.12.1	**Provozní postupy a zodpovědnosti**	
A.12.1.1	Dokumentované provozní postupy	**Ano**
A.12.1.2	Řízení změn	**Ano**
A.12.1.3	Řízení kapacit	**Ano**
A.12.1.4	Princip oddělení prostředí vývoje, testování a provozu	**Ano**
A.12.2	**Ochrana proti malwaru**	
A.12.2.1	Opatření proti malwaru	**Ano**
A.12.3	**Zálohování**	
A.12.3.1	Zálohování informací	**Ano**
A.12.4	**Zaznamenávání formou logů a monitorování**	
A.12.4.1	Zaznamenávání událostí formou logů	**Ano**
A.12.4.2	Ochrana logů	**Ano**
A.12.4.3	Logy o činnosti administrátorů a operátorů	**Ano**
A.12.4.4	Synchronizace hodin	**Ano**
A.12.5	**Správa provozního softwaru**	
A.12.5.1	Instalace softwaru na provozní systémy	**Ano**
A.12.6	**Řízení technických zranitelností**	
A.12.6.1	Řízení technických zranitelností	**Ano**
A.12.6.2	Omezení instalace softwaru	**Ano**
A.12.7	**Hlediska auditu informačních systémů**	
A.12.7.1	Opatření k auditu informačních systémů	**Ano**
A.13 Bezpečnost komunikací		
A.13.1	**Správa bezpečnosti sítě**	
A.13.1.1	Opatření v sítích	**Ano**
A.13.1.2	Bezpečnost síťových služeb	**Ano**
A.13.1.3	Princip oddělení v sítích	**Ano**
A.13.2	**Přenos informací**	
A.13.2.1	Politiky a postupy při přenosu informací	**Ano**
A.13.2.2	Dohody o přenosu informací	**Ano**
A.13.2.3	Elektronické předávání zpráv	**Ano**
A.13.2.4	Dohody o utajení nebo o mlčenlivosti	**Ano**

A.14 Akvizice, vývoj a údržba systémů		
A.14.1	**Bezpečnostní požadavky informačních systémů**	
A.14.1.1	Analýza a specifikace požadavků na bezpečnost informací	**Ano**
A.14.1.2	Zabezpečení aplikačních služeb ve veřejných sítích	**Ano**
A.14.1.3	Ochrana transakcí aplikačních služeb	**Ne**
A.14.2	**Bezpečnost v procesech vývoje a podpory**	
A.14.2.1	Politika bezpečného vývoje	**Ano**
A.14.2.2	Postupy řízení změn systému	**Ano**
A.14.2.3	Technické přezkoumání aplikací po změnách provozní platformy	**Ano**
A.14.2.4	Omezení změn softwarových balíků	**Ano**
A.14.2.5	Principy budování bezpečných systémů	**Ano**
A.14.2.6	Prostředí bezpečného vývoje	**Ano**
A.14.2.7	Outsourcovaný vývoj	**Ano**
A.14.2.8	Testování bezpečnosti systémů	**Ano**
A.14.2.9	Testování akceptace systémů	**Ano**
A.14.3	**Data pro testování**	
A.14.3.1	Ochrana dat pro testování	**Ano**
A.15 Dodavatelské vztahy		
A.15.1	**Bezpečnost informací v dodavatelských vztazích**	
A.15.1.1	Politika bezpečnosti informací pro dodavatelské vztahy	**Ano**
A.15.1.2	Bezpečnostní požadavky v dohodách s dodavateli	**Ano**
A.15.1.3	Dodavatelský řetězec informačních a komunikačních technologií	**Ne**
A.15.2	**Řízení dodávek služeb dodavatelů**	
A.15.2.1	Monitorování a přezkoumávání služeb dodavatelů	**Ano**
A.15.2.2	Řízení změn ve službách dodavatelů	**Ano**
A.16 Řízení incidentů bezpečnosti informací		
A.16.1	**Řízení incidentů bezpečnosti informací a zlepšování**	
A.16.1.1	Odpovědnosti a postupy	**Ano**
A.16.1.2	Hlášení událostí bezpečnosti informací	**Ano**
A.16.1.3	Hlášení slabých míst bezpečnosti informací	**Ano**
A.16.1.4	Posouzení a rozhodnutí o událostech bezpečnosti informací	**Ano**
A.16.1.5	Reakce na incidenty bezpečnosti informací	**Ano**
A.16.1.6	Ponaučení z incidentů bezpečnosti informací	**Ano**
A.16.1.7	Shromažďování důkazů	**Ano**
A.17 Aspekty řízení kontinuity činností organizace z hlediska bezpečnosti informací		
A.17.1	**Kontinuita bezpečnosti informací**	
A.17.1.1	Plánování kontinuity informační bezpečnosti	**Ano**
A.17.1.2	Implementace kontinuity bezpečnosti informací	**Ano**
A.17.1.3	Verifikace, přezkoumání a vyhodnocení kontinutiy bezpečnosti informací	**Ano**
A.17.2	**Redundance**	
A.17.2.1	Dostupnost vybavení pro zpracování informací	**Ano**
A.18 Soulad s požadavky		
A.18.1	**Soulad s právními a smluvními požadavky**	
A.18.1.1	Identifikace odpovídající legislativy a smluvních požadavků	**Ano**
A.18.1.2	Ochrana duševního vlastnictví	**Ano**
A.18.1.3	Ochrana záznamů	**Ano**
A.18.1.4	Soukromí a ochrana osobních informací	**Ano**
A.18.1.5	Regulace kryptografických opatření	**Ano**
A.18.2	**Přezkoumání bezpečnosti informací**	
A.18.2.1	Nezávislá přezkoumání bezpečnosti informací	**Ano**
A.18.2.2	Shoda s bezpečnostními politikami a normami	**Ano**
A.18.2.3	Přezkoumání technické shody	**Ano**