

## Prohlášení o aplikovatelnosti ISMS

Kapitola normy	Názvy kapitol přílohy "A" normy ČSN EN ISO 27001:2014	Opatření je zahrnut o	Důvod vyloučení prvku normy
<b>A.5</b>	<b>Politiky bezpečnosti informací</b>		
<b>A.5.1</b>	<b>Směřování bezpečnosti informací vedením organizace</b>		
Cíl:	Poskytnout nasměrování ze strany managementu a podporu informační bezpečnosti podle požadavků byznysu a příslušných zákonů a předpisů		
A.5.1.1	Politiky pro bezpečnost informací	Ano	
A.5.1.2	Přezkoumání politik pro bezpečnost informací	Ano	
<b>A.6</b>	<b>Organizace bezpečnosti informací</b>		
<b>A.6.1</b>	<b>Interní organizace</b>		
Cíl:	Nastavit rámec vedení pro zahájení a řízení implementace a provozování informační bezpečnosti v organizaci		
A.6.1.1	Role a odpovědnosti bezpečnosti informací	Ano	
A.6.1.2	Princip oddělení povinností	Ano	
A.6.1.3	Kontakt s příslušnými orgány a autoritami	Ano	
A.6.1.4	Kontakt se zájmovými skupinami	Ano	
A.6.1.5	Bezpečnost informací v řízení projektů	Ano	
<b>A.6.2</b>	<b>Mobilní zařízení a práce na dálku</b>		
Cíl:	Cíl: Zajistit bezpečnost při použití mobilních zařízení a pro práci na dálku		
A.6.2.1	Politika mobilních zařízení	Ano	
<b>A.6.2.2</b>	Práce na dálku	<b>Ne</b>	Organizace neumožňuje zaměstnancům ani dodavatelům vzdálený přístup
<b>A.7</b>	<b>Bezpečnost lidských zdrojů</b>		
<b>A.7.1</b>	<b>Před vznikem pracovního vztahu</b>		
Cíl:	Cíl: Zajistit, aby zaměstnanci a smluvní strany byli srozuměni se svými povinnostmi a aby pro jednotlivé role byli vybráni vhodní kandidáti		
A.7.1.1	Prověřování	Ano	
A.7.1.2	Podmínky pracovního vztahu	Ano	
<b>A.7.2</b>	<b>Během pracovního vztahu</b>		
Cíl:	Zajistit, aby si zaměstnanci a smluvní strany byli vědomi a plnili si svoje povinnosti v oblasti BI		
A.7.2.1	Odpovědnosti vedení organizace	Ano	
A.7.2.2	Povědomí, vzdělání a školení bezpečnosti informací	Ano	
A.7.2.3	Disciplinární řízení	Ano	
<b>A.7.3</b>	<b>Ukončení a změna pracovního vztahu</b>		
Cíl:	Chránit zájmy organizace v procesu změny nebo ukončení pracovního vztahu.		
A.7.3.1	Odpovědnosti při ukončení nebo změně pracovního vztahu	Ano	
<b>A.8</b>	<b>Řízení aktiv</b>		
<b>A.8.1</b>	<b>Odpovědnost za aktiva</b>		
Cíl:	Identifikovat aktiva organizace a definovat odpovědnosti k jejich přiměřené ochraně		
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	
<b>A.8.2</b>	<b>Klasifikace informací</b>		
Cíl:	Zajistit, aby informace získaly odpovídající úroveň ochrany v souladu s jejich důležitostí pro organizaci		
A.8.2.1	Klasifikace informací	Ano	
A.8.2.2	Označování informací	Ano	
A.8.2.3	Manipulace s aktivy	Ano	
<b>A.8.3</b>	<b>Manipulace s médii</b>		
Cíl:	Předcházet neoprávněnému vyjádření, modifikaci, odstranění nebo zničení informací uložených na médiích		
A.8.3.1	Správa výměnných médií	Ano	
A.8.3.2	Likvidace médií	Ano	
A.8.3.3	Přeprava fyzických médií	Ano	
<b>A.9</b>	<b>Řízení přístupu</b>		
<b>A.9.1</b>	<b>Požadavky organizace na řízení přístupu</b>		

Cíl:	Omezit přístup k informacím a vybavení pro zpracování informací	
A.9.1.1	Politika řízení přístupu	Ano
A.9.1.2	Přístup k sítím a síťovým službám	Ano
<b>A.9.2 Řízení přístupu uživatelů</b>		
Cíl:	Zajistit oprávněný přístup k informacím a předcházet neoprávněnému přístupu k systémům a službám	
A.9.2.1	Registrace a zrušení registrace uživatele	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
<b>A.9.3 Odpovědnosti uživatelů</b>		
Cíl:	Učinit uživatele odpovědné za ochranu jejich autentizačních informací	
A.9.3.1	Používání tajných autentizačních informací	Ano
<b>A.9.4 Řízení přístupu k systému a aplikacím</b>		
Cíl:	Předcházet neautorizovanému přístupu k systémům a aplikacím	
A.9.4.1	Omezení přístupu k informacím	Ano
A.9.4.2	Bezpečné postupy přihlášení	Ano
A.9.4.3	Systém správy hesel	Ano
A.9.4.4	Používání privilegovaných programových nástrojů	Ano
A.9.4.5	Řízení přístupu ke zdrojovým kódům programů	Ano
<b>A.10 Kryptografie</b>		
<b>A.10.1 Kryptografická opatření</b>		
Cíl:	Zajistit řádné a efektivní užívání kryptografie k ochraně důvěrnosti, autentičnosti a / nebo integrity informací	
A.10.1.1	Politika používání kryptografických opatření	Ano
A.10.1.2	Správa klíčů	Ano
<b>A.11 Fyzická bezpečnost a bezpečnost prostředí</b>		
<b>A.11.1 Bezpečné oblasti</b>		
Cíl:	Předcházet neautorizovanému fyzickému přístupu, poškození a zásahům do informací a vybavení pro zpracování informací organizace	
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
<b>A.11.2 Zařízení</b>		
Cíl:	Předcházet ztrátě, poškození, krádeži nebo kompromitaci aktiv a přerušení činnosti organizace	
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
<b>A.12 Bezpečnost provozu</b>		
<b>A.12.1 Provozní postupy a odpovědnosti</b>		
Cíl:	Zajistit správný a bezpečný provoz vybavení pro zpracování informací	
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
<b>A.12.2 Ochrana proti malwaru</b>		
Cíl:	Zajistit, aby informace a vybavení pro zpracování informací byly chráněny proti malwaru	
A.12.2.1	Opatření proti malwaru	Ano

<b>A.12.3 Zálohování</b>		
Cíl:	Chránit proti ztrátě dat	
A.12.3.1	Zálohování informací	Ano
<b>A.12.4 Zaznamenávání formou logů a monitorování</b>		
Cíl:	Zaznamenávat události a vytvářet záznamy	
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
<b>A.12.5 Správa provozního software</b>		
Cíl:	Zajistit integritu provozních systémů	
A.12.5.1	Instalace software na provozní systémy	Ano
<b>A.12.6 Řízení technických zranitelností</b>		
Cíl:	Zabránit využívání technických zranitelností	
A.12.6.1	Řízení technických zranitelností	Ano
A.12.6.2	Omezení instalace softwaru	Ano
<b>A.12.7 Hlediska auditu informačních systémů</b>		
Cíl:	Minimalizovat dopady auditních činností na provozní systémy	
A.12.7.1	Opatření k auditu informačních systémů	Ano
<b>A.13 Bezpečnost komunikací</b>		
<b>A.13.1 Správa bezpečnosti sítě</b>		
Cíl:	Zajistit ochranu informací v sítích a jejich podpůrných prostředcích pro zpracování informací	
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
<b>A.13.2 Přenos informací</b>		
Cíl:	Zajistit bezpečnost informací při jejich přenosu v rámci organizace a s externími subjekty	
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
<b>A.14 Akvizice, vývoj a údržba informačních systémů</b>		
<b>A.14.1 Bezpečnostní požadavky informačních systémů</b>		
Cíl:	Zajistit, aby se BI stala nedílnou součástí IS v jejich celém životním cyklu. To zahrnuje i požadavky na IS, které poskytují služby na informačních sítích.	
A.14.1.1	Analýza a specifikace požadavků bezpečnosti informací	Ano
A.14.1.2	Zabezpečení aplikačních služeb na veřejných sítích	Ano
A.14.1.3	Ochrana transakcí informačních služeb	Ano
<b>A.14.2 Bezpečnost v procesech vývoje a podpory</b>		
Cíl:	Zajistit, aby bezpečnost informací byla navrhována a implementována v životním cyklu vývoje informačních systémů	
A.14.2.1	Politika bezpečného vývoje	Ano
A.14.2.2	Postupy řízení změn systémů	Ano
A.14.2.3	Technické přezkoumání aplikací po změnách provozní platformy	Ano
A.14.2.4	Omezení změn softwarových balíčků	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
<b>A.14.3 Data pro testování</b>		
Cíl:	Zajistit ochranu dat používaných pro testování	
A.14.3.1	Ochrana dat pro testování	Ano
<b>A.15 Dodavatelské vztahy</b>		
<b>A.15.1 Bezpečnost informací v dodavatelských vztazích</b>		
Cíl:	Zajistit ochranu aktiv organizace, ke kterým mají dodavatelé přístup	
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 Ano

#### **A.15.2 Řízení dodávek služeb dodavatelů**

Cíl: Udržovat dohodnutou úroveň bezpečnosti informací a dodávky služeb ve shodě s dodavatelskými dohodami

A.15.2.1 Monitorování a přezkoumání 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**

Cíl: Zajistit odpovídající a efektivní přístup ke zvládnání incidentů bezpečnosti informací, zahrnující komunikaci ohledně bezpečnostních událostí a slabých míst

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 činnosti organizace z hlediska bezpečnosti informací**

##### **A.17.1 Kontinuita informační bezpečnosti**

Cíl: Kontinuita bezpečnosti informací musí být součástí systémů řízení kontinuity činnosti organizace

A.17.1.1 Plánování kontinuity bezpečnosti informací Ano

A.17.1.2 Implementace kontinuity bezpečnosti informací Ano

A.17.1.3 Verifikace, přezkoumání a vyhodnocování kontinuity bezpečnosti Ano

##### **A.17.2 Redundance**

Cíl: Zajistit dostupnost vybavení pro zpracování informací

A.17.2.1 Dostupnost vybavení pro práci s informacemi Ano

#### **A.18 Soulad s požadavky**

##### **A.18.1 Soulad s právními a smluvními požadavky**

Cíl: Vyvarovat se porušení zákonných, předpisových nebo smluvních povinností týkajících se bezpečnosti informací a na jakýchkoli bezpečnostních požadavků

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 údajů Ano

A.18.1.5 Regulace kryptografických opatření Ano

##### **A.18.2 Přezkoumání informační bezpečnosti**

Cíl: Zajistit, že bezpečnost informací je implementována a provozována v souladu s politikami a postupy organizace

A.18.2.1 Nezávislé přezkoumání bezpečnosti informací Ano

A.18.2.2 Shoda s bezpečnostními politikami a normami Ano

A.18.2.3 Přezkoumání technické shody Ano