Prohlášení o aplikovatelnosti

pro třetí strany

Vlastník dokumentu:	Chief Privacy and Security Officer	Označení dokumentu: Verze dokumentu:	OD-006 2.0
Schválil:	Ondřej Synovec CEO	Verze platná k: 23.1. 2025	*El. podpis*

Obsah

1 Prohlášení o aplikovatelnosti opatření

Na základě přezkoumání rizik bezpečnosti informací a stavu opatření k jejich snížení generální ředitel vydává toto prohlášení o aplikovatelnosti bezpečnostních opatření dle doporučení normy ČSN EN ISO/IEC 27001:2023 příloha A včetně rozšíření ČSN ISO/IEC 27017:2017 příloha A (mezinárodní verze norem: EN ISO/IEC 27001:2022, ISO/IEC 27017:2015), dále jen ISO 27001 a ISO 27017.

Stav aplikace opatření byl vyhodnocen ke dni 10.1. 2025.

1.1 Oblast a rozsah působnosti ISMS a BCMS

Prohlášení o aplikovatelnosti je platné v následujícím rozsahu působnosti systému řízení bezpečnosti informací (ISMS) a zajištění kontinuity činností (BCMS):

Oblast působnosti ISMS a BCMS zahrnuje ochranu informací a zajištění kontinuity činností souvisejících s návrhem, vývojem, provozem a poskytováním cloudové aplikační platformy Signi.com, která poskytuje služby pro tvorbu a oběh dokumentů, jejich digitálního podepisování a důvěryhodné archivace.

Vzhledem k rozsahu a obsahu poskytovaných služeb je stanovena oblast působnosti ISMS a BCMS tak, aby pokrývala celou organizaci, žádné její organizační složky tedy z působení tohoto systému ISMS a BCMS nejsou vyňaty. Tím bude zajištěno, že všechny služby, nebo interní činnosti budou komplexně i jakoukoli svou částí řízeny systémem ISMS a BCMS a nebudou se mu vymykat.

1.2 Kritéria výběru opatření

Jednotlivá opatření ke snížení rizik byla vybrána na základě výstupů analýzy rizika a dopadů. K aplikaci byla doporučena ochranná opatření, pro rizika dosahující úrovně rizik 3 a výše na škále 1 až 4, tak aby se tato snížila na akceptovatelnou úroveň, tj. na úroveň 2 a méně.

Při návrhu opatření byla upřednostňována řešení, která by umožňovala pokrýt co nejvíce rizik pomocí interních zdrojů. Současně byla brána v úvahu již existující a plánovaná opatření.

1.3 Vyloučená opatření

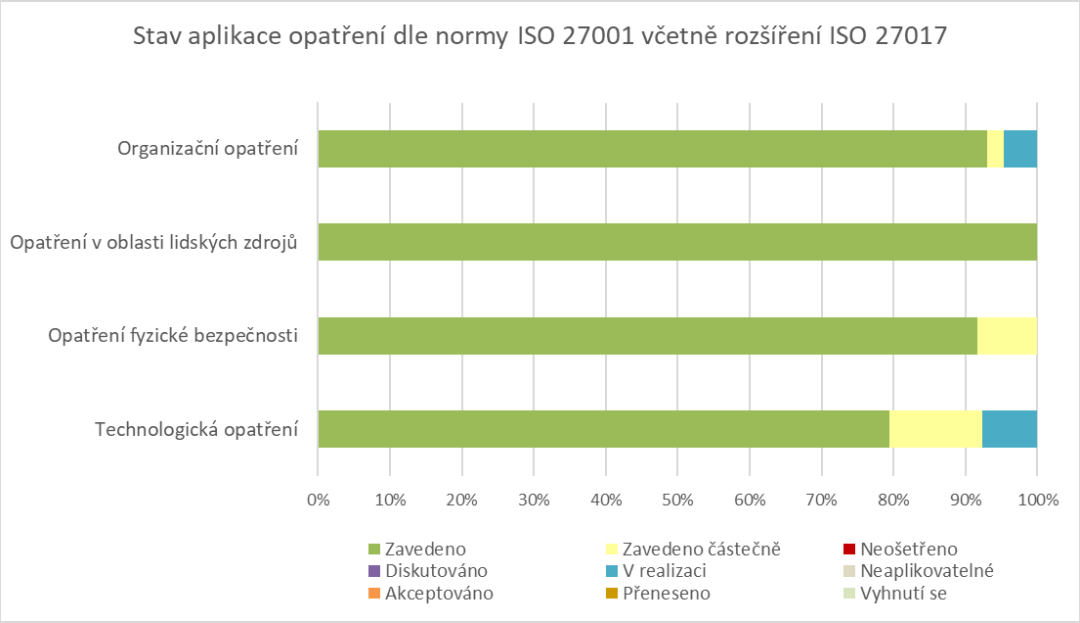
Z opatření informační bezpečnosti uvedených v ISO 27001 příloha A a rozšířeného souboru opatření cloudových služeb ISO 27017 příloha A bylo vyloučeno následující opatření:

8.11 Maskování dat

Z důvodu, že společnost Digital factory s.r.o. nezpracovává žádná data, kde by bylo vhodné nebo požadované jejich maskování.

1.4 Stav aplikace vybraných opatření

Souhrnný přehled stavu aplikace opatření informační bezpečnosti dle požadavků normy ISO 27001 uvedených v příloze A včetně rozšíření ISO 27017 příloha A je uveden na Obr. 1.



Obr. 1. Souhrnný přehled stavu bezpečnostních opatření

Stav aplikace vybraných opatření ke snížení rizik byl hodnocen dle následujících kritérií.

Kritéria pro hodnocení stavu opatření ke snížení rizik	
Zavedeno	Opatření je aplikováno.
Zavedeno částečně	Opatření je aplikováno částečně (nejsou splněny všechny požadavky).
Neošetřeno	O způsobu řešení rizika ještě nebylo rozhodnuto.
Diskutováno	Je zvažována implementace opatření (existuje a projednává se návrh opatření, zadání projektu).
V realizaci	Probíhá realizace opatření.
Neaplikovatelné	Opatření není v prostředí společnosti aplikovatelné (nelze jej realizovat).
Akceptováno	Akceptována úroveň rizika.
Přeneseno	Riziko bylo přeneseno na třetí stranu (pojištění, outsourcing, …).
Vyhnutí se	Společnost se vyhnula riziku (ukončení rizikové činnosti, změna lokality, změna technologie, náhrada rizikového systému jiným, např: LINUX namísto Win ...)

Tab. 1. Kritéria pro hodnocení stavu vybraných opatření

V následující Tab. 2 je uvedeno detailní vyhodnocení stavu bezpečnostních opatření doporučených k implementaci normou ISO 27001 Příloha A (respektive normou ISO 27002) včetně rozšíření o doporučení normy ISO 27017.

Opatření informační bezpečnosti ČSN ISO/IEC 27001:2023 - Příloha A (normativní) včetně rozšíření ČSN ISO/IEC 27017:2017			
Ref. ISO	**Opatření**	**Vybráno k realizaci**	**Aktuální stav opatření**
5	**Organizační opatření**		
5.1	Politiky pro informační bezpečnost	Ano	Zavedeno
5.2	Role a odpovědnosti v oblasti informační bezpečnosti	Ano	Zavedeno
5.3	Oddělení povinností	Ano	Zavedeno
5.4	Odpovědnosti vedení	Ano	Zavedeno
5.5	Kontakt s autoritami	Ano	Zavedeno
5.6	Kontakt se zvláštními zájmovými skupinami	Ano	Zavedeno
5.7	Zpravodajství o hrozbách	Ano	Zavedeno
5.8	Informační bezpečnost v řízení projektů	Ano	Zavedeno
5.9	Evidence informací a dalších souvisejících aktiv	Ano	Zavedeno
5.10	Přípustné používání informací a dalších souvisejících aktiv	Ano	Zavedeno
5.11	Vrácení aktiv	Ano	Zavedeno
CLD.8.1.5	Odstranění aktiv zákazníka cloudových služeb		
CLD.8.1.5	Odstranění aktiv zákazníka cloudových služeb (Zákazník Cloud služeb)	Ano	Zavedeno
CLD.8.1.5	Odstranění aktiv zákazníka cloudových služeb (Poskytovatel Cloud služeb)	Ano	Zavedeno
5.12	Klasifikace informací	Ano	Zavedeno
5.13	Označování informací	Ano	Zavedeno
5.14	Předávání informací	Ano	Zavedeno
5.15	Řízení přístupu	Ano	Zavedeno
5.16	Management identit	Ano	Zavedeno
5.17	Autentizační informace	Ano	Zavedeno
5.18	Přístupová práva	Ano	Zavedeno
5.19	Informační bezpečnost ve vztazích s dodavateli	Ano	Zavedeno
5.20	Řešení informační bezpečnosti v dohodách s dodavateli	Ano	Zavedeno
5.21	Management informační bezpečnosti v dodavatelském řetězci ICT	Ano	Zavedeno
5.22	Monitorování, přezkoumávání a management změn dodavatelských služeb	Ano	Zavedeno
5.23	Informační bezpečnost při používání cloudových služeb	Ano	Zavedeno
5.24	Plánování a příprava managementu incidentů informační bezpečnosti	Ano	Zavedeno
5.25	Posuzování a rozhodování o událostech informační bezpečnosti	Ano	V realizaci
5.26	Odezva na incidenty informační bezpečnosti	Ano	V realizaci
5.27	Poučení se z incidentů informační bezpečnosti	Ano	Zavedeno
5.28	Shromažďování důkazů	Ano	Zavedeno částečně
5.29	Informační bezpečnost během narušení	Ano	Zavedeno
5.30	Připravenost ICT na zajištění kontinuity činnosti organizace	Ano	Zavedeno
5.31	Zákonné, statutární, regulatorní a smluvní požadavky	Ano	Zavedeno
5.32	Práva duševního vlastnictví	Ano	Zavedeno
5.33	Ochrana záznamů	Ano	Zavedeno
5.34	Soukromí a ochrana PII	Ano	Zavedeno
5.35	Nezávislé přezkoumání Informační bezpečnosti	Ano	Zavedeno
5.36	Dodržování politik, pravidel a norem pro informační bezpečnost	Ano	Zavedeno
5.37	Dokumentované provozní postupy	Ano	Zavedeno

Opatření informační bezpečnosti ČSN ISO/IEC 27001:2023 - Příloha A (normativní) včetně rozšíření ČSN ISO/IEC 27017:2017			
Ref. ISO	**Opatření**	**Vybráno k realizaci**	**Aktuální stav opatření**
CLD.6.3	Vztah mezi zákazníkem cloudových služeb a poskytovatelem cloudových služeb		
CLD.6.3.1	Sdílené role a odpovědnosti v rámci prostředí cloud computingu (Zákazník Cloud služeb)	Ano	Zavedeno
CLD.6.3.1	Sdílené role a odpovědnosti v rámci prostředí cloud computingu (Poskytovatel Cloud služeb)	Ano	Zavedeno
CLD.12.1.5	Provozní bezpečnostní administrace		
CLD.12.1.5	Provozní bezpečnostní administrace (Zákazník Cloud služeb)	Ano	Zavedeno
CLD.12.1.5	Provozní bezpečnostní administrace (Poskytovatel Cloud služeb)	Ano	Zavedeno
6	**Opatření v oblasti lidských zdrojů**		
6.1	Prověřování	Ano	Zavedeno
6.2	Podmínky pracovního poměru	Ano	Zavedeno
6.3	Povědomí, vzdělávání a školení o informační bezpečnosti	Ano	Zavedeno
6.4	Disciplinární řízení	Ano	Zavedeno
6.5	Odpovědnosti po ukončení nebo změně pracovního poměru	Ano	Zavedeno
6.6	Dohody o důvěrnosti nebo mlčenlivosti	Ano	Zavedeno
6.7	Práce na dálku	Ano	Zavedeno
6.8	Podávání zpráv o událostech informační bezpečnosti	Ano	Zavedeno
7	**Opatření fyzické bezpečnosti**		
7.1	Perimetry fyzické bezpečnosti	Ano	Zavedeno
7.2	Fyzický vstup	Ano	Zavedeno
7.3	Zabezpečení kanceláří, místností a vybavení	Ano	Zavedeno
7.4	Monitorování fyzické bezpečnosti	Ano	Zavedeno
7.5	Ochrana před fyzickými a přírodními hrozbami	Ano	Zavedeno
7.6	Práce v zabezpečených oblastech	Ano	Zavedeno
7.7	Prázdný stůl a prázdná obrazovka	Ano	Zavedeno
7.8	Umístění a ochrana zařízení	Ano	Zavedeno
7.9	Bezpečnost aktiv mimo prostory organizace	Ano	Zavedeno
7.10	Paměťová média	Ano	Zavedeno částečně
7.11	Podpůrné služby	Ano	Zavedeno
7.12	Bezpečnost kabelových rozvodů	Ano	Zavedeno
7.13	Údržba zařízení	Ano	---
7.14	Bezpečná likvidace nebo opakované použití zařízení	Ano	---
8	**Technologická opatření**		
8.1	Koncová zařízení uživatele	Ano	Zavedeno
8.2	Privilegovaná přístupová práva	Ano	Zavedeno
8.3	Omezení přístupu k informacím	Ano	Zavedeno
8.4	Přístup ke zdrojovému kódu	Ano	Zavedeno
8.5	Bezpečná autentizace	Ano	Zavedeno
8.6	Management kapacit	Ano	Zavedeno
8.7	Ochrana před škodlivým softwarem	Ano	Zavedeno
8.8	Management technických zranitelností	Ano	Zavedeno částečně
8.9	Management konfigurací	Ano	V realizaci

Opatření informační bezpečnosti ČSN ISO/IEC 27001:2023 - Příloha A (normativní) včetně rozšíření ČSN ISO/IEC 27017:2017			
Ref. ISO	**Opatření**	**Vybráno k realizaci**	**Aktuální stav opatření**
8.10	Vymazání informací	Ano	Zavedeno
8.11	Maskování dat	Ne	---
8.12	Prevence úniku dat	Ano	Zavedeno částečně
8.13	Zálohování informací	Ano	Zavedeno
8.14	Redundance vybavení pro zpracování informací	Ano	Zavedeno
8.15	Zaznamenávání formou logů	Ano	Zavedeno částečně
8.16	Monitorovací činnosti	Ano	Zavedeno částečně
8.17	Synchronizace hodin	Ano	Zavedeno
CLD.12.4.5	Monitorování cloudových služeb		
CLD.12.4.5	Monitorování cloudových služeb (Zákazník Cloud služeb)	Ano	Zavedeno
CLD.12.4.5	Monitorování cloudových služeb (Poskytovatel Cloud služeb)	Ano	Zavedeno
8.18	Používání privilegovaných obslužných programů	Ano	Zavedeno
8.19	Instalace softwaru na provozních systémech	Ano	Zavedeno
8.20	Bezpečnost sítí	Ano	Zavedeno
8.21	Bezpečnost síťových služeb	Ano	Zavedeno částečně
8.22	Oddělení sítí	Ano	Zavedeno
CLD.13.1.4	Koordinace správy bezpečnosti virtuálních a fyzických sítí (Poskytovatel Cloud služeb)	Ano	Zavedeno
8.23	Filtrování webových stránek	Ano	Zavedeno
8.24	Používání kryptografie	Ano	Zavedeno
8.25	Životní cyklus bezpečného vývoje	Ano	Zavedeno
8.26	Požadavky na bezpečnost aplikací	Ano	Zavedeno
8.27	Principy architektury a inženýrství bezpečných systémů	Ano	V realizaci
8.28	Bezpečné programování	Ano	V realizaci
8.29	Testování bezpečnosti při vývoji a akceptaci	Ano	Zavedeno
8.30	Vývoj zajišťovaný externími zdroji	Ano	Zavedeno
8.31	Oddělení prostředí vývoje, testování a produkce	Ano	Zavedeno
8.32	Management změn	Ano	Zavedeno
8.33	Informace pro testování	Ano	Zavedeno
8.34	Ochrana informačních systémů během auditního testování	Ano	Zavedeno
CLD.9.5	Řízení přístupu k datům zákazníka cloudových služeb ve sdíleném virtuálním prostředí		
CLD.9.5.1	Oddělení ve virtuálním výpočetním prostředí (Poskytovatel Cloud služeb)	Ano	Zavedeno
CLD.9.5.2	Zodolnění virtuálního stroje (Zákazník Cloud služeb)	Ano	Zavedeno
CLD.9.5.2	Zodolnění virtuálního stroje (Poskytovatel Cloud služeb)	Ano	Zavedeno

Tab. 2. Detailní vyhodnocení stavu bezpečnostních opatření