# Prohlášení o aplikovatelnosti

## 1 ÚČEL A ROZSAH ZPRÁVY

Účelem tohoto dokumentu je návrh způsobu zvládání rizik v souladu s požadavky:

a) Systém managementu bezpečnosti informací, které vyplývají z mezinárodního standardu, kterým je rodina norem ISO/IEC 27000.

Cílem a účelem prohlášení o aplikovatelnosti (dále také „PoA“), je vytvoření přehledu přijatých bezpečnostních opatření, která popisují jednotlivé oblasti informačního systému společnosti Škoda ICT s.r.o. (dále také „ŠICT“) a ohodnocení úrovně splnění požadavků na bezpečnost informací.

| ISO/IEC 27001:2022 | | | | |
|---|---|---|---|---|
| **ID** | **Název opatření** | **Popis opatření** | **Aplikováno bezp. opatření** | **Odůvodnění neaplikování bezp. opatření** |
| 5.1 | Politiky pro informační bezpečnost | Politika a informační bezpečnosti a tematicky specifické politiky musí být definovány, schváleny vedením, zveřejněn, sděleny a vzaty na vědomí příslušnými pracovníky a zainteresovanými stranami a přezkoumávány v plánovaných intervalech a v případě významných změn. | ANO | |
| 5.2 | Role a odpovědnosti v oblasti informační bezpečnosti | Role a odpovědnosti v oblasti informační bezpečnosti musí být definovány a přiděleny podle potřeb organizace. | ANO | |
| 5.3 | Oddělení povinností | Protichůdné povinnosti a protichůdné oblasti odpovědnosti musí být odděleny. | ANO | |
| 5.4 | Odpovědnosti vedení | Vedení musí vyžadovat, aby všichni pracovníci uplatňovali informační bezpečnost v souladu s vytvořenou politikou informační bezpečnosti, tematicky specifickými politikami a postupy organizace. | ANO | |
| 5.5 | Kontakt s autoritami | Organizace musí navázat a udržovat kontakt s příslušnými autoritami. | ANO | |
| 5.6 | Kontakt se zvláštními zájmovými skupinami | Organizace musí navázat a udržovat kontakty se zvláštními zájmovými skupinami nebo jinými odbornými fóry v oblasti bezpečnosti a profesními sdruženími. | ANO | |
| 5.7 | Zpravodajství o hrozbách | Informace týkající se hrozeb pro informační bezpečnost musí být shromažďovány a analyzovány tak, aby poskytovaly informace o hrozbách. | ANO | |
| 5.8 | Informační bezpečnost v řízení projektů | Informační bezpečnost být integrována do řízení projektů. | ANO | |
| 5.9 | Evidence informací a dalších souvisejících aktiv | Musí být vytvořen a udržován inventář informací a dalších souvisejících aktiv, včetně vlastníků. | ANO | |
| 5.10 | Přípustné používání | Musí být identifikována, dokumentována a zavedena pravidla | ANO | |

| ISO/IEC 27001:2022 | | | | |
|---|---|---|---|---|
| **ID** | **Název opatření** | **Popis opatření** | **Aplikováno bezp. opatření** | **Odůvodnění neaplikování bezp. opatření** |
| | informací a dalších souvisejících aktiv | pro přípustné používání informací a dalších souvisejících aktiv a postupy pro nakládání s nimi. | | |
| 5.11 | Vrácení aktiv | Pracovníci a případně další zainteresované strany musí po změně nebo ukončení pracovního poměru, smlouvy nebo dohody vrátit veškerá aktiva organizace, která mají k dispozici. | ANO | |
| 5.12 | Klasifikace informací | Informace, musí být klasifikovány podle potřeb organizace v oblasti informační bezpečnosti na základě důvěrnosti, integrity, dostupnosti a požadavků příslušných zainteresovaných stran. | ANO | |
| 5.13 | Označování informací | Musí být vypracován vhodný soubor postupů pro označování informací a zaveden v souladu se systémem klasifikace informací přijatým organizací. | ANO | |
| 5.14 | Předávání informací | Pravidla, postupy nebo dohody pro předávání informací v organizaci a mezi organizacemi a mezi dalšími stranami musí být zavedeny pro všechny typy přenosových zařízení. | ANO | |
| 5.15 | Řízení přístupu | Pravidla pro řízení fyzického a logického přístupu k informacím a dalším souvisejícím aktivům musí být vytvořena a zavedena na základě požadavků vyplývajících z činnosti organizace a požadavků na informační bezpečnost. | ANO | |
| 5.16 | Management identit | Musí být řízen celý životní cyklus identit. | ANO | |
| 5.17 | Autentizační informace | Přidělování a management autentizačních informací musí být řízeny řídícím procesem, včetně poradenství pracovníkům ohledně vhodného zacházení s autentizačními informacemi. | ANO | |
| 5.18 | Přístupová práva | Přístupová práva k informacím a dalším souvisejícím aktivům musí být poskytována, přezkoumávána, upravována a odebírána v souladu | ANO | |

| ISO/IEC 27001:2022 | | | | |
|---|---|---|---|---|
| **ID** | **Název opatření** | **Popis opatření** | **Aplikováno bezp. opatření** | **Odůvodnění neaplikování bezp. opatření** |
| | | s tematicky specifickou politikou organizace a pravidly pro řízení přístupu. | | |
| 5.19 | Informační bezpečnost ve vztazích s dodavateli | Musí být definovány a zavedeny procesy a postupy pro management rizik informační bezpečnosti spojených s používáním produktů nebo služeb dodavatele. | ANO | |
| 5.20 | Řešení informační bezpečnosti v dohodách s dodavateli | Příslušné požadavky na informační bezpečnost musí být stanoveny a dohodnuty s každým dodavatelem na základě typu dodavatelského vztahu. | ANO | |
| 5.21 | Management informační bezpečnosti v dodavatelském řetězci ICT | Musí být definovány a zavedeny procesy a postupy pro management rizik informační bezpečnosti spojených s dodavatelským řetězcem produktů a služeb ICT. | ANO | |
| 5.22 | Monitorování, přezkoumávání a management změn dodavatelských služeb | Organizace musí pravidelně monitorovat, přezkoumávat, vyhodnocovat a řídit změny v postupech informační bezpečnosti dodavatelů a v poskytování služeb dodavateli. | ANO | |
| 5.23 | Informační bezpečnost při používání cloudových služeb | Procesy pro získání, používání, management a ukončení cloudových služeb musí být ustaveny v souladu s požadavky organizace na informační bezpečnost. | ANO | |
| 5.24 | Plánování a příprava managementu incidentů informační bezpečnosti | Organizace musí plánovat a připravit se na management incidentů informační bezpečnosti definováním, ustavením a sdělením procesů, rolí a odpovědností v oblasti managementu incidentů informační bezpečnosti. | ANO | |
| 5.25 | Posuzování a rozhodování o událostech informační bezpečnosti | Organizace musí posoudit události informační bezpečnosti a rozhodnout, zda mají být klasifikovány jako incidenty informační bezpečnosti. | ANO | |
| 5.26 | Odezva na incidenty informační bezpečnosti | Na incidenty informační bezpečnosti se musí reagovat v souladu s dokumentovanými postupy. | ANO | |

| ISO/IEC 27001:2022 | | | | |
|---|---|---|---|---|
| **ID** | **Název opatření** | **Popis opatření** | **Aplikováno bezp. opatření** | **Odůvodnění neaplikování bezp. opatření** |
| 5.27 | Poučení se z incidentů informační bezpečnosti | Poznatky získané z incidentů informační bezpečnosti musí být využity k posílení a zlepšení opatření informační bezpečnosti. | ANO | |
| 5.28 | Shromažďování důkazů | Organizace musí stanovit a zavést postupy pro identifikaci, shromažďování, získávání a uchování důkazů souvisejících s událostmi informační bezpečnosti. | ANO | |
| 5.29 | Informační bezpečnost během narušení | Organizace musí naplánovat, jak udržovat informační bezpečnost na odpovídající úrovni během narušení. | ANO | |
| 5.30 | Připravenost ICT na zajištění kontinuity činnosti organizace | Připravenost ICT musí být plánována, zavedena, udržována a testována na základě cílů kontinuity činností organizace a požadavků na kontinuitu ICT. | ANO | |
| 5.31 | Zákonné, statutární, regulatorní a smluvní požadavky | Zákonné, statutární, regulatorní a smluvní požadavky týkající se informační bezpečnosti a přístup organizace ke splnění těchto požadavků musí být identifikovány, dokumentovány a udržovány aktuální. | ANO | |
| 5.32 | Práva duševního vlastnictví | Organizace musí zavést vhodné postupy na ochranu práv duševního vlastnictví. | ANO | |
| 5.33 | Ochrana záznamů | Záznamy musí být chráněny před ztrátou, zničením, falšováním, neoprávněným přístupem a neoprávněným uvolněním. | ANO | |
| 5.34 | Soukromí a ochrana PII | Organizace musí identifikovat a splnit požadavky týkající se zachování soukromí a ochrany PII v souladu s platnými zákony a předpisy a smluvními požadavky. | ANO | |
| 5.35 | Nezávislé přezkoumání Informační bezpečnosti | Přístup organizace k managementu informační bezpečnosti a jejím implementacím četně lidí, procesů a technologií musí být nezávisle přezkoumávány v plánovaných intervalech nebo v případě významných změn. | ANO | |

| ISO/IEC 27001:2022 | | | | |
|---|---|---|---|---|
| **ID** | **Název opatření** | **Popis opatření** | **Aplikováno bezp. opatření** | **Odůvodnění neaplikování bezp. opatření** |
| 5.36 | Dodržování politik, pravidel a norem pro informační bezpečnost | Dodržování politik informační bezpečnosti organizace, tematicky specifických politik, pravidel a standardů musí být pravidelně přezkoumáváno. | ANO | |
| 5.37 | Dokumentované provozní postupy | Provozní postupy pro vybavení pro zpracování informací musí být zdokumentovány a zpřístupněny pracovníkům, kteří je potřebují. | ANO | |
| 6.1 | Prověřování | Prověřování minulosti všech uchazečů, kteří se chtějí stát pracovníky, musí být prováděno před nástupem do organizace a průběžně s ohledem na platné zákony, předpisy a etiku a mělo by být úměrné požadavkům vyplývajícím z činnosti organizace, klasifikaci informací, které mají být zpřístupněny, a vnímaným rizikům. | ANO | |
| 6.2 | Podmínky pracovního poměru | V pracovních smlouvách musí být uvedena odpovědnost pracovníků a organizace za informační bezpečnost. | ANO | |
| 6.3 | Povědomí, vzdělávání a školení o informační bezpečnosti | Pracovníci organizace a příslušné zainteresované strany musí získat odpovídající povědomí, vzdělávání a školení o informační bezpečnosti a pravidelné aktualizace politiky informační bezpečnosti organizace, tematicky specifických politik a postupů, které jsou relevantní pro jejich pracovní funkci. | ANO | |
| 6.4 | Disciplinární řízení | Musí být formalizován a oznámen disciplinární postup pro přijímání opatření vůči pracovníkům a dalším příslušným zainteresovaným stranám, které se dopustily porušení politiky informační bezpečnosti. | ANO | |
| 6.5 | Odpovědnosti po ukončení nebo změně pracovního poměru | Odpovědnost a povinnosti v oblasti informační bezpečnosti, které zůstávají v platnosti i po ukončení nebo změně pracovního poměru, musí být definovány, prosazovány a sdělovány příslušným pracovníkům a dalším zainteresovaným stranám. | ANO | |

| ISO/IEC 27001:2022 | | | | |
|---|---|---|---|---|
| **ID** | **Název opatření** | **Popis opatření** | **Aplikováno bezp. opatření** | **Odůvodnění neaplikování bezp. opatření** |
| 6.6 | Dohody o důvěrnosti nebo mlčenlivosti | Musí být identifikovány, zdokumentovány, pravidelně přezkoumávány a podepsány pracovníky a dalšími příslušnými zainteresovanými stranami dohody o důvěrnosti nebo mlčenlivosti, které odrážejí potřeby organizace v oblasti ochrany informací. | ANO | |
| 6.7 | Práce na dálku | Pokud pracovníci pracují na dálku, musí být zavedena bezpečnostní opatření na ochranu informací, ke kterým se přistupuje, které se zpracovávají nebo ukládají mimo prostory organizace. | ANO | |
| 6.8 | Podávání zpráv o událostech informační bezpečnosti | Organizace musí pracovníkům poskytnout mechanismus pro včasné podávání zpráv o pozorovaných nebo podezřelých událostech informační bezpečnosti prostřednictvím příslušných kanálů. | ANO | |
| 7.1 | Perimetry fyzické bezpečnosti | Musí být definovány bezpečnostní perimetry a používány k ochraně oblastí, které obsahují informace a další související aktiva. | ANO | |
| 7.2 | Fyzický vstup | Zabezpečené oblasti musí být na vstupu a přístupových místech chráněny vhodnými opatřeními. | ANO | |
| 7.3 | Zabezpečení kanceláří, místností a vybavení | Musí být navržena a zavedena opatření pro fyzickou bezpečnost kanceláří, místností a vybavení. | ANO | |
| 7.4 | Monitorování fyzické bezpečnosti | Prostory musí být nepřetržitě monitorovány pro neoprávněný fyzický vstup. | ANO | |
| 7.5 | Ochrana před fyzickými a přírodními hrozbami | Musí být navržena a zavedena ochrana před fyzickými a přírodními hrozbami, jako jsou přírodní katastrofy a jiné úmyslné či neúmyslné fyzické hrozby vůči infrastruktuře. | ANO | |
| 7.6 | Práce v zabezpečených oblastech | Musí být navržena a zavedena bezpečnostní opatření pro práci v zabezpečených oblastech. | ANO | |

| ISO/IEC 27001:2022 | | | | |
|---|---|---|---|---|
| **ID** | **Název opatření** | **Popis opatření** | **Aplikováno bezp. opatření** | **Odůvodnění neaplikování bezp. opatření** |
| 7.7 | Prázdný stůl a prázdná obrazovka | U vybavení pro zpracování informací musí být stanovena a náležitě vynucována pravidla prázdného stolu pro papírová média a přenosná paměťová média a pravidla prázdné obrazovky. | ANO | |
| 7.8 | Umístění a ochrana zařízení | Zařízení musí být bezpečně umístěno a chráněno. | ANO | |
| 7.9 | Bezpečnost aktiv mimo prostory organizace | Aktiva mimo prostory organizace musí být chráněna. | ANO | |
| 7.10 | Paměťová média | S paměťovými médii se musí nakládat v průběhu jejich životního cyklu pořízení, používání, přepravy a likvidace v souladu s klasifikačním schématem organizace a požadavky na nakládání s nimi. | ANO | |
| 7.11 | Podpůrné služby | Zařízení pro zpracování informací musí být chráněna před výpadky napájení a jinými poruchami způsobenými selháním podpůrných služeb. | ANO | |
| 7.12 | Bezpečnost kabelových rozvodů | Kabely přenášející napájení, data nebo podpůrné informační služby musí být chráněny před odposlouchávání, rušením nebo poškozením. | ANO | |
| 7.13 | Údržba zařízení | Zařízení musí být správně udržováno, aby byla zajištěna dostupnost, integrita a důvěrnost informací. | ANO | |
| 7.14 | Bezpečná likvidace nebo opakované použití zařízení | Části zařízení obsahující paměťová média musí být prověřeny s cílem zajistit, aby byla před likvidací nebo opakovaném použití odstraněna nebo bezpečně přepsána všechna citlivá data a licencovaný software. | ANO | |
| 8.1 | Koncová zařízení uživatele | Informace uložené na koncových zařízeních uživatele, zpracovávané těmito zařízeními nebo přístupné prostřednictvím těchto zařízení musí být chráněny. | ANO | |

| ISO/IEC 27001:2022 | | | | |
|---|---|---|---|---|
| **ID** | **Název opatření** | **Popis opatření** | **Aplikováno bezp. opatření** | **Odůvodnění neaplikování bezp. opatření** |
| 8.2 | Privilegovaná přístupová práva | Přidělování a používání privilegovaných přístupových práv musí být omezeno a řízeno. | ANO | |
| 8.3 | Omezení přístupu k informacím | Přístup k informacím a dalším souvisejícím aktivům musí být omezen v souladu s ustavenou tematicky specifikou politikou řízení přístupu. | ANO | |
| 8.4 | Přístup ke zdrojovému kódu | Přístup pro čtení a zápis ke zdrojovému kódu, vývojovým nástrojům a softwarovým knihovnám musí být náležitě řízen. | ANO | |
| 8.5 | Bezpečná autentizace | Technologie a postupy bezpečné autentizace musí být implementovány na základě omezení přístupu k informacím a tematicky specifické politiky řízení přístupu. | ANO | |
| 8.6 | Management kapacit | Využívání zdrojů být monitorováno a upravováno v souladu se současnými a očekávanými požadavky na kapacity. | ANO | |
| 8.7 | Ochrana před škodlivým software | Ochrana před škodlivým softwarem musí být implementována a podporována odpovídajícím povědomím uživatelů. | ANO | |
| 8.8 | Management technických zranitelností | Musí být získány informace o technických zranitelnostech používaných informačních systémů, musí být vyhodnoceno vystavení organizace těmto zranitelnostem a musí být přijata vhodná opatření. | ANO | |
| 8.9 | Management konfigurací | Konfigurace, včetně konfigurací bezpečnosti hardwaru, software, služeb a sítí, musí být ustaveny, dokumentovány, implementovány, monitorovány a přezkoumávány. | ANO | |
| 8.10 | Vymazání informací | Informace uložené v informačních systémech, zařízeních nebo na jiných paměťových médiích musí být vymazány, pokud již nejsou potřebné. | ANO | |
| 8.11 | Maskování dat | Maskování dat musí být používáno v souladu s tematicky specifickou politikou organizace týkající se řízení | ANO | |

| ISO/IEC 27001:2022 | | | | |
|---|---|---|---|---|
| **ID** | **Název opatření** | **Popis opatření** | **Aplikováno bezp. opatření** | **Odůvodnění neaplikování bezp. opatření** |
| | | přístupu a dalšími souvisejícími tematicky specifickými politikami a požadavky vyplývajícími z činnosti organizace, přičemž je třeba vzít v úvahu platnou legislativu. | | |
| 8.12 | Prevence úniku dat | Opatření pro prevenci úniku dat musí být aplikována na systémy, sítě a jakákoliv další zařízení, která zpracovávají, ukládají nebo přenášejí citlivé informace. | ANO | |
| 8.13 | Zálohování informací | Záložní kopie informací, softwaru a systémů musí být udržovány a pravidelně testovány v souladu se schválenou tematicky specifickou politikou zálohování. | ANO | |
| 8.14 | Redundance vybavení pro zpracování informací | Vybavení pro zpracování informací musí být implementováno s dostatečnou redundancí, aby byly splněny požadavky na dostupnost. | ANO | |
| 8.15 | Zaznamenávání formou logů | Musí být vytvářeny, uchovávány, chráněny a analyzovány logy, které zaznamenávají činností, výjimky, poruchy a další relevantní události. | ANO | |
| 8.16 | Monitorovací činnost | Sítě, systémy a aplikace musí být monitorovány z hlediska anomálního chování a musí být přijata vhodná opatření k vyhodnocení potenciálních incidentů informační bezpečnosti. | ANO | |
| 8.17 | Synchronizace hodin | Hodiny systémů zpracování informací používaných organizací musí být synchronizovány se schválenými zdroji času. | ANO | |
| 8.18 | Používání privilegovaných obslužných programů | Používání obslužných programů, které mohou být schopné potlačit systémová a aplikační opatření, musí být omezeno a přísně kontrolováno. | ANO | |
| 8.19 | Instalace software na provozních systémech | Musí být zavedeny postupy a opatření pro bezpečný management instalace softwaru v provozních systémech. | ANO | |
| 8.20 | Bezpečnost sítí | Sítě a síťová zařízení musí být zabezpečeny, řízeny a kontrolovány, | ANO | |

| ISO/IEC 27001:2022 | | | | |
|---|---|---|---|---|
| **ID** | **Název opatření** | **Popis opatření** | **Aplikováno bezp. opatření** | **Odůvodnění neaplikování bezp. opatření** |
| | | aby byly chráněny informace v systémech a aplikacích. | | |
| 8.21 | Bezpečnost síťových služeb | Musí být identifikovány, zavedeny a monitorovány bezpečnostní mechanismy, úrovně služeb a požadavky na síťové služby. | ANO | |
| 8.22 | Oddělení sítí | Skupiny informačních služeb, uživatelů a informačních systémů musí být v sítích organizace odděleny. | ANO | |
| 8.23 | Filtrování webových stránek | Přístup na externí webové stránky musí být řízen tak, aby se omezilo vystavení se škodlivému obsahu. | ANO | |
| 8.24 | Používání kryptografie | Musí být definována a zavedena pravidla pro efektivní používání kryptografie, včetně managementu kryptografických klíčů. | ANO | |
| 8.25 | Životní cyklus bezpečného vývoje | Musí být ustavena a uplatňována pravidla pro bezpečný vývoj softwaru a systémů. | ANO | |
| 8.26 | Požadavky na bezpečnost aplikací | Při vývoji nebo pořizování aplikací musí být identifikovány, specifikovány a schváleny požadavky na informační bezpečnost. | ANO | |
| 8.27 | Principy architektury a inženýrství bezpečných systémů | Principy inženýrství bezpečných systémů musí být stanoveny, dokumentovány, udržovány a uplatňovány při všech činnostech vývoje informačního systému. | ANO | |
| 8.28 | Bezpečné programování | Při vývoji softwaru se musí uplatňovat zásady bezpečného programování. | ANO | |
| 8.29 | Testování bezpečnosti při vývoji a akceptaci | Procesy testování bezpečnosti musí být definovány a zavedeny v rámci životního cyklu vývoje. | ANO | |
| 8.30 | Vývoj zajišťovaný externími zdroji | Organizace musí řídit, monitorovat a přezkoumávat činnosti související s vývojem systému zajišťovaným externími zdroji. | ANO | |
| 8.31 | Oddělení prostředí vývoje, testování a produkce | Vývojová, testovací a produkční prostředí musí být oddělena a zabezpečena. | ANO | |

| ISO/IEC 27001:2022 | | | | |
|---|---|---|---|---|
| **ID** | **Název opatření** | **Popis opatření** | **Aplikováno bezp. opatření** | **Odůvodnění neaplikování bezp. opatření** |
| 8.32 | Management změn | Změny vybavení pro zpracování informací a informačních systémů musí být předmětem postupů managementu změn. | ANO | |
| 8.33 | Informace pro testování | Informace pro testování musí být vhodně vybrány, chráněny a spravovány. | ANO | |
| 8.34 | Ochrana informačních systémů během auditního testování | Auditní testy a další ověřovací činnosti zahrnující posouzení provozních systémů musí být naplánovány a odsouhlaseny testovací entitou a příslušným vedením. | ANO | |