Vyhlášení politiky informační a kybernetické bezpečnosti a ustanovení systému firmy icMK s.r.o.

OBSAH:

1. Úvodní ustanovení

1.1. Účel

Účelem dokumentu je v souladu s požadavky správy informačního a kybernetického prostoru ustanovit bezpečnostní politiky v oblasti systému řízení kybernetické a informační bezpečnosti ve společnosti icMK s.r.o..

Stanovení politik se vztahuje k současným podnikatelským aktivitám a je aplikováno i na služby poskytované externími dodavateli.

1.2. Rozsah závaznosti

Tento dokument je určen pro všechny zaměstnance společnosti jejichž seznam je zdokumentován v Záznamech o provedeném školení zaměstnanců.

Politika bezpečnosti informací je zpřístupněna relevantním zainteresovaným stranám při podpisu smlouvy. Za její předání je odpovědný podepisující pracovník. Dále je uveřejněna na webu icMK s.r.o.

1.3. Vyhlášení systému řízení bezpečnosti informací

Tímto dokumentem vyhlašuje jednatel společnosti icMK s.r.o. politiku bezpečnosti informací.

Hlavním cílem společnosti je zajištění kybernetické a informační bezpečnosti pomocí přiměřených opatření tak, abych byla eliminována rizika spojená s chodem společnosti, zajištěna ochranu aktiv pro poskytování bezpečné a spolehlivé služby zákazníkům a splnění požadavků na IKB všech zainteresovaných stran které jsou definovány ve smlouvách nebo dané zákonem.

Tento cíl je naplňován vybudováním a neustálým zlepšováním systému řízení informační a kybernetické bezpečnosti a řízením rizik v kontextu podnikatelských aktivit společnosti.

Informační bezpečnost je komplex opatření, který zahrnuje proces navrhování, schvalování a implementaci softwarových, hardwarových, technických, personálních ochranných opatření spojených s minimalizací možných ztrát, vzniklých v důsledku poškození, zničení nebo zneužití informačních systémů.

Pojmem Kybernetická bezpečnost rozumíme souhrn všech právních, organizačních, technických a vzdělávacích prostředků společnosti směřujících k zajištění ochrany prvků aktiv a jednotného kybernetického prostoru.

Systém řízení kybernetické bezpečnosti je nastaven tak, aby respektoval požadavky právních předpisů, relevantních norem, standardů a doporučení a v neposlední řadě také bezpečnostní požadavky zúčastněných stran, především našich zákazníků.

Všude, kde je potřeba, implementujeme přiměřená bezpečnostní opatření. K posouzení přiměřenosti bezpečnostních opatření využíváme proces řízení rizik.

Naplňujeme jednotlivé bezpečnostní cíle pomocí adekvátních opatření určených procesem řízení rizik v souladu s legislativními požadavky.

Aktivními kroky zvyšujeme bezpečnostní povědomí zaměstnanců.

Vedení společnosti se zavazuje politiky a standardy dodržovat a bude jejich praktickou aplikaci podporovat a rozhodovat

S ohledem na analýzu rizik se vedení společnosti zavazuje plnit všechny vydané dokumenty, aktivně reálný stav kontrolovat, chránit, revidovat a zdokonalovat a dále se zavazuje kontrolovat dodržování vydaných dokumentů a směrnic všemi zaměstnanci.

Firma používá informační entity: dokumenty, směrnice a záznamy.

1.4. Odpovědnosti

Za seznámení zaměstnanců s dokumenty ISO 27001 odpovídá jednatel icMK s.r.o..

Registr a analýzu rizik zpracoval a každoročně reviduje manažer informační bezpečnosti, který zároveň realizuje opatření vedoucí k trvalému zlepšování úrovně bezpečnosti informací.

Vazby mezi jednotlivými pracovními pozicemi ve společnosti jsou dány Organigramem.

2.Systém a politika bezpečnosti informací

Při budování informační a kybernetické bezpečnosti zohledňujeme a respektujeme tyto požadavky, potřeby a pravidla:

- legislativy České republiky a EU
- přiměřeně zajistit ochranu obchodního tajemství a dalších důvěrných informací, plnění smluvních požadavků a závazků
- přiměřeně chránit oprávněné zájmy třetích stran
- zájmů společnosti, obchodních a interních procesů s ohledem na dostupnost a integritu informací

2.1 Předpoklady pro budování systému pro zlepšování ochrany bezpečnosti informací

- zajištění

- nepřetržitého zdokonalování systému řízení kybernetické a informační bezpečnosti, v souladu s požadavky této politiky.
- konsolidace bezpečnostních funkcí a bezpečnostních aplikací a jejich postupné zlepšování a zefektivňování.
- odpovědnosti všech zaměstnanců za kybernetickou a informační bezpečnost v rozsahu jejich pracovní náplně a jejich odpovědností a kompetencí.
- detekce, eskalaci a zvládnutí bezpečnostních incidentů s důrazem na prevenci.

- dostupnosti kritických informačních systémů společnosti i v případě náhlého výpadku implementací procesu řízení kontinuity činností.
- efektivní řízení přístupu k informacím, informačním systémům a technologiím tak, aby byla zajištěna přiměřená úroveň jejich důvěrnosti.
- podmínek pro bezpečné umístnění důležitých technologických komponent a zajistit jejich fyzickou i technologickou ochranu a ochranu před vlivy okolního prostředí.
- bezpečnosti a spolehlivosti užívaných systémů a aplikací využíváním všech jejich bezpečnostních funkcí a vlastností.
- zvyšování bezpečnostního povědomí zaměstnanců, odběratelů našich služeb a vést je ke zlepšování úrovně bezpečnosti a dodržování bezpečnostních zásad.
- bezpečného vývoje aplikací.

- implementace

- systému řízení a zajištění souladu kybernetické a informační bezpečnosti s interními předpisy, metodikou a platnou legislativou České republiky
- nejlepších zkušenosti v oblasti řízení kybernetické a informační bezpečnosti
- politiky informační bezpečnosti s cílem vytvořit předpoklady pro zajištění přiměřené úrovně kybernetické a informační bezpečnosti.
- bezpečnostních požadavků do zákaznických projektů.
- vhodných a přiměřených bezpečnostních opatření s přihlédnutím k využití procesu řízení rizik

2.2 Cíle v oblasti systému kybernetické a informační bezpečnosti

Hlavním cílem firmy v oblasti kybernetické a informační bezpečnosti je zachování dostupnosti, důvěrnosti a integrity služeb a to vlastních, klientských či třetích smluvních stran.

Základní principy

- zajištění

- dodržování všech normativů: dokumentů, zákonů, směrnic, souvisejících legislativních norem
- dodržování vzdělávání a školení informační a kybernetické bezpečnosti
- dodržování kontrolních a vyhodnocovacích procesů
- zachování provozní schopnosti a spolehlivosti společnosti
- nedopuštění diskreditace zákazníků společnosti a tím i diskreditaci společnosti samotné
- ochrany informačních aktiv proti poškození, zničení, odcizení, ztrátě, nedovolenému přístupu datům a jejich změně

- bezpečného vývoje aplikací

Přístup k cílům

Dosažení cílů musí být reálné, měřitelné a termínované, frekvenčně kontrolovatelné a vyhodnocované a dokumentované. Společnost při definování cílů musí postupovat v souladu s těmito pravidly:

- srozumitelnost a jasný popis
- přímá vazba na zvýšení bezpečnosti aktiv ve společnosti
- odpovídat potřebám pracovníka, pro kterého je určen
- stanovení doby, dokdy je vytčeného cíle třeba dosáhnout
- jasná definice kdo za splnění cílů odpovídá

Hlavní cíle určuje a navrhuje manažer informační bezpečnosti ve spolupráci s vedením společnosti na základě schváleného ročního plánu. V případě přeplánování v průběhu aktuálního roku mohou být změněny i cíle informační a kybernetické bezpečnosti.

Zdroje potřebné k naplnění cílů musí být zahrnuty ve schváleném firemním rozpočtu. Za plnění cílů jsou následně zodpovědní přiděleni zaměstnanci, nebo a vlastníci procesů / aktiv.

Vyhodnocování se provádí ve frekvenci, kterou určuje vlastník procesu / aktiva (minimálně jednou ročně).

V případě negativního vývoje plnění cílů je vlastník příslušného procesu odpovědný za přijetí nápravných / preventivních opatření.

3. Kybernetická a informační bezpečnost – rozsah a hranice systému řízení

3.1 Základní oblasti informačního systému společnosti

Zahrnují služby, postupy, nástroje a prostředky:

- určené pro podporu činností společnosti, včetně podpory činností v rámci stavu informačního nebezpečí podle ISO 27001
- spojené s výměnou informací mezi společností a dalšími orgány veřejné moci či soukromoprávními subjekty
- spojené s prezentováním informací o společnosti a poskytováním informací široké veřejnosti

3.2 Fyzické lokality

Systém řízení kybernetické a informační bezpečnosti zahrnuje tuto fyzickou lokalitu spol. icMK s.r.o.:

- sídlo firmy

- lokality a objekty smluvních partnerů a třetích stran vycházejících z obchodních vztahů s IcMK s.r.o., viz příslušné smlouvy.

3.3 Informační systémy

a) v rozsahu systému řízení kybernetické bezpečnosti jsou zařazeny všechny informační systémy, které firma provozuje, včetně systémů testovacích, vývojových a dalších neprodukčních systémů.
b) v rozsahu systému řízení kybernetické bezpečnosti nejsou zařazeny žádné významné informační systémy podle zákona č. 181/2014 Sb. nebo podle zákona č. 412/2005 Sb.
c) ochrana dat a informací je odvozena od požadavků a znění smluv se zákazníky a platné právní úpravy. Ve smlouvách je nutné stanovit, zdali je nutné přijmout na straně zákazníka zvýšenou úroveň zabezpečení nebo zda lze takovou úroveň zajistit v rámci poskytované služby.

3.4 Zainteresované strany

Mezi důležité zainteresované strany patří:

- Zákazníci společnosti a dodavatelé společnosti.
- Zaměstnanci společnosti.
- Statutární zástupci společnosti, majitelé společnosti
- Orgány a osoby, kterým se ukládají povinnosti v oblasti informační bezpečnosti, podle §3 Zákona č. 181/2014Sb.
- Úřad na ochranu osobních údajů.
- Ministerstvo průmyslu a obchodu.
- Ministerstvo vnitra.
- Finanční úřad.
- Česká správa sociálního zabezpečení.
- Osoby a uživatelé, které provedly hlášení informačního bezpečnostního incidentu.

3.5 Dodavatelé a závislosti

Společnost icMK s.r.o. je nezávislá na dodávkách zásadních služeb nezbytných pro své fungování. Rozsah služeb je definován smlouvami.

4. Pravidla a postupy pro řízení dokumentace

Za každý dokument (politiku) procesu Kybernetické a informační bezpečnosti odpovídá manažer informační bezpečnosti, který se řídí těmito činnostmi:

- ukládáním, zachováním a čitelností dokumentu
- dostupností a použitelností
- zajištění jeho pravidelné aktualizace a řízení změn např. řízení verzováním
- likvidací dokumentu

4.1 Pravidla a postupy pro řízení zdrojů a provozu systému řízení kybernetické a informační bezpečnosti

Vedení společnosti deklaruje svou podporu při řízení a přerozdělování finančních, personálních, organizačních i technických zdrojů potřebných pro správné řízení a funkčnost procesů kybernetické a informační bezpečnosti.

Zdroje potřebné pro ustanovení, implementování, udržování a neustálé zlepšování systému řízení kybernetické a informační bezpečnosti musí být uvedeny ve firemním plánu nebo v zadání jednotlivých rozvojových projektů.

Manažer informační bezpečnosti je odpovědný za efektivní a uvážlivé použití zdrojů.

4.2 Odpovědnost za procesy kybernetické a informační bezpečnosti

Kompetence jednotlivých rolí, které se podílejí na systému řízení kybernetické a informační bezpečnosti musí být určeny. Podrobnosti jsou určeny v kapitole 8.

Spolehlivé fungování systémů řízení kybernetické a informační bezpečnosti závisí na vytvoření a obsazení rolí, které převezmou jednotlivé úkoly a zajistí jejich plnění v rámci realizovaných činností. Důležitým faktorem je přidělení dostatečných pravomocí a odpovědností za kybernetickou a informační bezpečnost pro definované role.

Za dodržování zásad kybernetické a informační bezpečnosti odpovídají všichni zaměstnanci v rozsahu své pracovní náplně a svých odpovědností a kompetencí.

Vedoucí zaměstnanci na jednotlivých úrovních řízení odpovídají za výkon kontrolních funkcí v rozsahu své působnosti. Konkrétní povinnosti a pravomoci jsou definovány v rámci souvisejících jednotlivých bezpečnostních politik.

4.3 Řízení výjimek

Všechny výjimky vůči plnění politik a stanovených postupů řízení kybernetické a informační bezpečnosti musí být schváleny manažerem informační bezpečnosti. Žadatel musí poskytnout podrobné vysvětlení důvodů pro schválení výjimky.

Výjimka může být schválena na přesně stanovené časové období. Každé prodloužení výjimky musí být přezkoumáno a projednáno a schváleno vedením společnosti.

Manažer informační bezpečnosti je odpovědný za zaznamenání všech výjimek v evidenci výjimek.

Evidence výjimek musí obsahovat:

- identifikace žadatele o výjimku
- vysvětlení, proč není možné pravidla dodržovat a je nutná výjimka
- identifikace bezpečnostních pravidel, která není možné dodržovat
- stanovení časového období, na které je výjimka schválená
- dočasná opatření, která omezují nežádoucí dopady

Manažer informační bezpečnosti je odpovědný za přezkoumání všech výjimek bez zbytečného odkladu a ve spolupráci s žadatelem musí připravit efektivní plán na řešení výjimky, který bude součástí plánu zvládání rizik a naplnění cílů kybernetické a informační bezpečnosti.

5. Pravidla a postupy pro provádění auditů informační bezpečnosti

Audity informační bezpečnosti musí být prováděny v souladu s programem auditů informační bezpečnosti. Získávají informace o tom, zda systém řízení bezpečnosti informací vyhovuje požadavkům stanovených bezpečnostními politikami a standardy systému řízení bezpečnosti informací a požadavkům normy ČSN ISO/IEC 27001 a zda je systém implementován a udržován.

5.1 Program a provádění auditů informační bezpečnosti

Manažer informační bezpečnosti musí:

- plánovat, ustavit, implementovat a udržovat program auditů informační bezpečnosti, včetně četnosti, metod, odpovědnosti, plánování požadavků a podávání zpráv.

Program auditů informační bezpečnosti musí obsahovat následující informace:

- kritéria a rozsah všech auditů informační bezpečnosti, plánovaný čas všech auditů informační bezpečnosti.

Program auditů informační bezpečnosti musí brát v úvahu důležitost aktiv a procesů zahrnutých do rozsahu systému řízení bezpečnosti informací, výsledky hodnocení a zvládání rizik a výsledky předchozích auditů. Program auditů informační bezpečnosti je připravován na období tří let a všechna důležitá aktiva musí být během tohoto období alespoň jednou prověřena.

Program auditů informační bezpečnosti musí být odsouhlasen manažerem informační bezpečnosti.

Auditor informační bezpečnosti musí:

- provádět audity při zajištění objektivity a nestrannosti procesu auditu,

- znát politiky, standardy a požadavky bezpečnosti informací, které jsou pro audit informační bezpečnosti podstatné

- provádět všechny činnosti auditu informační bezpečnosti profesionálně a sbírat důkazy, které se vztahují k nálezům auditu informační bezpečnosti a nálezy auditu informační bezpečnosti řádně dokumentovat.

- na základě programu auditů informační bezpečnosti připravit plán auditu informační bezpečnosti

- projednat plán auditu informační bezpečnosti s auditovanou společností, a to nejméně dva týdny před plánovaným termínem auditu

- koordinovat všechny činnosti během auditu informační bezpečnosti

shromažďovat nálezy informační bezpečnosti a tyto nálezy kategorizovat

- objasnit nálezy a výsledky auditu informační bezpečnosti na závěrečném setkání s představiteli auditovaných

- připravit zprávu z auditu informační bezpečnosti a požádat představitele auditovaných o její schválení

- předat schválenou zprávu z auditu informační bezpečnosti představitelům auditovaného, manažerovi informační bezpečnosti

5.2 základní kategorizace zjištění - nálezů z auditu informační a kybernetické bezpečnosti

kritické - systémová neshoda (CAT1), *vysoké* - nesystémová neshoda (CAT2), *střední* - pozorování (OBS), *nízké* - příležitost pro zlepšení (OFI)

Kritické - systémová neshoda: jako opakované či systematické neplnění požadavků normy či jiných závazných povinností případně neřešení méně významných neshod či jejich opakovaný výskyt musí být použita v následujících případech:

- absence jednoho nebo více požadovaných systémových prvků systému řízení bezpečnosti informací nebo situace, která může vznést významné pochyby, že informace nebo služby IT jsou dostatečně bezpečné.

- skupina méně významných neshod indikující neodpovídající implementaci nebo nedostatečnou efektivitu systému řízení bezpečnosti informací.

- méně významná neshoda, která přetrvává nebo nebyla řádně napravena, musí být překlasifikována na neshodu významnou.

Vysoké - nesystémová neshoda: dílčí neplnění požadavků či jiných závazných povinností v podobě jednotlivých selhání v disciplíně nebo kontrole během průběhu implementace či provozu požadavků, které neznamenají selhání celého systému řízení bezpečnosti informací nebo nevedou k zásadním pochybnostem, že informace nebo služby IT jsou dostatečně bezpečné. Celkově je systémový požadavek definován, implementován a vykazuje schopnosti být přiměřeně efektivní.

Střední - pozorování: není neshoda, ale odchylka od stanovených postupů, která by, pokud nebude řešena, mohla v budoucnosti vést k neplnění stanovených požadavků či jiných závazných povinností.

Nízké - příležitost ke zlepšení: možnosti pro zvýšení účinnosti a účelnosti prováděných činností organizace, které sice mohou splňovat minimální požadavky, ale které by mohly být vhodným způsobem zlepšeny. Příležitosti na zlepšování se mohou orientovat na zlepšení systému řízení bezpečnosti informací nebo jeho výkonnosti a většinou vycházejí ze zkušeností auditora, jeho znalostí, dobré praxe nebo porovnání používaných technik mezi pracovišti.

6. Pravidla a postupy pro přezkoumání systému řízení bezpečnosti informací

Hodnocení stavu a přiměřenosti ISŘ výkonným vedením firmy: jedním z podkladů k přezkoumání je zpráva bezpečnostního manažera a výsledky z interních auditů.

Dále zpětná vazba od zainteresovaných stran, výsledky posuzování rizik a vyhodnocení cílů.

Vlastníci aktiv a vedoucí zaměstnanci musí provádět pravidelné kontroly, jak jsou v rámci jejich odpovědnosti dodržována pravidla informační bezpečnosti a bezpečnostní politiky.

Výsledky přezkoumání shody s bezpečnostními politikami a normami musí být oznámeny manažerovi informační bezpečnosti, který je odpovědný za sumarizaci výsledků a jejich zahrnutí do přezkoumání systému řízení informační bezpečnosti vedením.

- Přezkoumání politik pro bezpečnost informací

Manažer informační bezpečnosti je odpovědný za přezkoumání a schválení vhodnosti a přiměřenosti bezpečnostních politik každé dva roky nebo po významné změně. Když je on nebo vlastník dokumentu odpovědný za vysvětlení pravidel a realizaci změn a požadavků stanovených bezpečnostními politikami, učiní tak plánovaným způsobem.

7. Pravidla a postupy pro nápravná opatření a zlepšování systému řízení bezpečnosti informací

Systém řízení bezpečnosti informací je postaven na principu PDCA cyklu (plánuj, dělej, zkontroluj, jednej), který je možné jinak definovat i jako proces neustálého zlepšování se.

Nápravná opatření a jejich související procesy jsou definovány v Příručce icMK a v dokumentu Registr a analýza rizik.

8. Politiky systému řízení bezpečnosti informací

Systém řízení bezpečnosti informací je složen z politik, které jsou obsaženy v dokumentu D3 Příručka icMK. V ní jsou politiky dále rozvedeny případně do podoby detailního dokumentu.

a) systém řízení kybernetické bezpečnosti
určuje základní postupy systému řízení kybernetické bezpečnosti jako je stanovení cílů kybernetické bezpečnosti, řízení dokumentace, provádění auditů informační bezpečnosti, provádění přezkoumání systému řízení kybernetické bezpečnosti a postupy pro zlepšování systému řízení kybernetické bezpečnosti.

b) organizační bezpečnost
určuje základní práva a povinnosti všech klíčových rolí, které se aktivně podílí na efektivním prosazování informační bezpečnosti.

c) řízení dodavatelů a dodavatelských řetězců
určuje pravidla a postupy pro přenesení povinností spojených s prosazováním informační bezpečnosti na smluvní dodavatele včetně pravidelného hodnocení angažovanosti dodavatelů.

d) identifikace, klasifikace a řízení aktiv
která zahrnuje pravidla pro bezpečné nakládání s aktivy, určuje přístupy, jak je možné aktiva kategorizovat z hlediska důvěrnosti, integrity a dostupnosti. Následně mohou být opatření informační bezpečnosti stanovena s ohledem na klasifikaci aktiv tak, aby se způsoby ochrany zjednodušily a standardizovaly

e) bezpečnost lidských zdrojů
určuje pravidla a postupy pro výběr zaměstnanců a smluvních partnerů a stanoví opatření pro rozvoj bezpečnostního povědomí.

f) řízení provozu a komunikací
určuje základní pravidla a postupy pro zajištění efektivního a bezpečného provozu informačních systémů.

g) řízení přístupu
určuje pravidla a postupy pro přidělování počítačových účtů a pro přidělování a kontrolu přístupových oprávnění k jednotlivým aktivům.

h) bezpečné chování uživatelů
je soubor pravidel informační bezpečnosti, která jsou spojena s uživateli a jejich chováním podporujícím opatření informační bezpečnosti.

i) zálohování a obnova
určuje pravidla a postupy spojené s pravidelným zálohováním a zajištěním pravidelného testování obnovitelnosti zálohovaných informací.

j) přenos a výměna dat a informací
určuje pravidla a postupy pro bezpečnou výměnu informací mezi lokalitami a s dalšími subjekty.

k) řízení technických zranitelností
určuje pravidla a postupy pro zjišťování známých zranitelností a jejich efektivní odstranění či minimalizaci případných negativních dopadů spojených se zranitelnostmi technických prostředků.

l) bezpečné používání mobilních zařízení a práce na dálku
určuje způsoby správného a bezpečného použití mobilních zařízení.

m) poskytování a nabývání licencí programového vybavení a informací

určuje pravidla a postupy spojená nabýváním a využíváním licencí programového vybavení.

n) dlouhodobé ukládání a archivace
určuje pravidla a postupy spojené s povinností archivace definovaných dokumentů a záznamů, a jsou v souladu s archivačním řádem.

o) fyzická bezpečnost a ochrana
určuje pravidla a postupu pro uplatňování fyzické ochrany informačních systémů a používaných technických aktiv.

p) bezpečnost ICT/ICS prostředků a sítě
určuje pravidla a postupy pro zajištění potřebné úrovně bezpečnosti lokálních i globálních komunikačních sítí.

q) ochrana před škodlivým kódem
určuje pravidla a postupy pro ochranu před škodlivými kódy a minimalizaci případných negativních dopadů spojených s projevy škodlivých kódů.

r) detekce kybernetických bezpečnostních událostí
určuje pravidla a postupy pro nasazení a efektivní využívání nástrojů, které dovolují odhalovat pokusy o neautorizované zneužití informačních systémů či služeb IT a zjišťovat pokusy o informační útoky a na tyto pokusy efektivně reagovat.

s) bezpečnost procesů vývoje, akvizice a podpory
určuje pravidla a postupy, které je nutné uplatnit v rámci životního cyklu vývoje pro zajištění potřebné úrovně bezpečnosti nově vyvíjených informačních systémů nebo služeb IT.

Pozn.: Systém řízení informační bezpečnosti se nevztahuje na informační systémy ve smyslu zákona č. 412/2005 Sb. o ochraně utajovaných informací a bezpečnostní způsobilosti, ve znění pozdějších předpisů.

t) řízení kontinuity činnosti

u) identifikace a hodnocení aktiv pro identifikaci, hodnocení a řízení rizik

v) ochrana osobních údajů
obsahuje charakteristiku zpracovávaných osobních údajů a určuje pravidla ochrany osobních údajů,

w) audit a kontrola

9. Vazby na dotčené závazné povinnosti

Nařízení Evropského Parlamentu a Rady (EU) 2016/679	o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů
Zákon č. 262/2006 Sb.	Zákoník práce
Zákon č. 90/2012 Sb.	Zákon o obchodních společnostech a družstvech (zákon o obchodních korporacích)
Zákon č. 89/2012 Sb.	Zákon občanský zákoník
Vyhláška č. 373/2016 Sb.	Vyhláška o předávání údajů do Národního zdravotnického informačního systému
Zákon č. 499/2004 Sb.	Zákon o archivnictví a spisové službě
Vyhláška 259/2012 Sb.	Vyhláška o podrobnostech výkonu spisové služby
Zákon č. 418/2011 Sb.	Zákon o trestní odpovědnosti právnických firem
Zákon č. 300/2008 Sb.	Zákon o elektronických úkonech a autorizované konverzi dokumentů
Vyhláška 193/2009 Sb.	Vyhláška o stanovení podrobností provádění autorizované konverze dokumentů
Zákon č. 480/2004 Sb.,	Zákon o některých službách informační společnosti
Zákon č. 563/1991 Sb.	Zákon o účetnictví (§ 31)
Zákon 523/1992 Sb.	Zákon daňovém poradenství a Komoře daňových poradců České republiky (§6 odst. 9)
Zákon č. 110/2019 Sb.	Zákon o zpracování osobních údajů
Zákon č. 253/2008 Sb.	Zákon o některých opatřeních proti legalizaci výnosů z trestné činnosti a financování terorismu
Bezúhonnost Zákon č. 269/1994 Sb.	Zákon o Rejstříku trestů
Zákon č. 40/2009 Sb.	Trestní zákoník
Zákon č. 227/2000 Sb.	Zákon o elektronickém podpisu
Zákon č. 106/1999 Sb.	Zákon o svobodném přístupu k informacím
Zákon č. 85/1996 Sb.	Zákon o advokacii
Zákon č. 412/2005 Sb.	Zákon o ochraně utajovaných informací a o bezpečnostní způsobilosti

Zákon č. 413/2005 Sb.	Zákon o změně zákonů v souvislosti s přijetím zákona o ochraně utajovaných informací a o bezpečnostní způsobilosti.
Nařízení vlády č. 522/2005 Sb.	Nařízení vlády, kterým se stanoví seznam utajovaných informací
Zákon 181/2014 Sb.	Zákon o kybernetické bezpečnosti (§ 3g, §8 bod 4, §161c a 2b)
Vyhláška 316/2014 Sb.	Vyhláška o kybernetické bezpečnosti
Vyhláška č. 82/2018 Sb.	Vyhláška o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat (vyhláška o kybernetické bezpečnosti)
Vyhláška 437/2017 Sb.	Vyhláška o kritériích pro určení provozovatele základní služby
Vyhláška 437/2017 Sb.	Vyhláška o významných informačních systémech a jejich určujících kritériích
Zákon 412/2005 Sb.	Zákon o ochraně utajovaných informací a o bezpečnostní způsobilosti
Vyhláška 529/2005 Sb.	Vyhláška o administrativní bezpečnosti a o registrech utajovaných informací
Zákon č. 127/2005 Sb.	Zákon o elektronických komunikacích
Zákon č. 634/1992 Sb.	Zákon o ochraně spotřebitele (§ 23odst. 17)
Zákon č. 251/2016 Sb.	Zákon o některých přestupcích (spor osoba vs osoba – např. kamery)
Zákon č. 297/2016 Sb.	Zákon o službách vytvářejících důvěru pro elektronické transakce
Zákon č. 480/2004 Sb.	Zákon o některých službách informační společnosti
Zákon č. 240/2000 Sb.	Zákon o krizovém řízení
Nařízení vlády č. 432/2011 Sb.	o kritériích pro určení prvku kritické infrastruktury (ve znění nařízení vlády č. 315/2014 Sb.)
Zákon č. 12/2020 Sb.	Zákon o právu na digitální služby
Zk. č. 239/2000 Sb.	o integrovaném záchranném systému a o změně některých zákonů
Zk. č. 240/2000 Sb.	o krizovém řízení a o změně některých zákonů
Zk. č. 241/2000 Sb.	o hospodářských opatřeních při krizových stavech
Zk. č. 110/2019 Sb.	Zákon o zpracování osobních údajů
Směrnice Evropského parlamentu a Rady (EU) 2022/2555	ze dne 14. prosince 2022 o opatřeních k zajištění vysoké společné úrovně kybernetické bezpečnosti v Unii a o změně nařízení (EU) č. 910/2014 a směrnice (EU) 2018/1972 a o zrušení směrnice (EU) 2016/1148 (směrnice NIS 2)

Zk. č. 226/2022 Sb.	Zákon, kterým se mění zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti), ve znění pozdějších předpisů
Vyhláška č. 479/2024 Sb.	upravuje informační bezpečnost
Vyhláška č. 447/2024 Sb.	zaměřuje se na zajištění kryptografické ochrany utajovaných informací
Nový zákon o kybernetické bezpečnosti	přijatý v roce 2025 míří nyní do Senátu, implementuje směrnici NIS2 a rozšiřuje regulaci na více organizací. Účinnost se očekává ve druhé polovině roku 2025.

Pozn.: uvedeny jsou dokumenty v platném znění k datu nabytí platnosti dokumentu a k datu jeho revize. Aktuální, konsolidované znění vnějších předpisů Sbírky zákonů ČR je k dispozici zde.

Počet stran: 15
Datum 1. vydání a nabytí účinnosti: 1. 1. 2025
Poslední revize: 1. 1. 2025
Záznamy o změnách v dokumentu, aktualizace: -

Zpracoval: Ing. Petr Muchna, manažer informační bezpečnosti

Schválil: Luboš Muchna, jednatel icMK s.r.o.