POLITIKA ISMS

Preambule

Závazek vedení

Vedení společnosti KOMAS spol. s r. o. (dále jen KOMAS) prohlašuje, že podporuje ustavení, zavedení, provoz, monitorování, přezkoumání, udržování a zlepšování systému řízení bezpečnosti informací v rámci společnosti, že bude garantem dodržování tohoto systému, bude propagovat význam jeho zavedení, udržování a zlepšování a bude ve spolupráci s ostatními vedoucími všech zúčastněných společností dbát na plnění povinností z něj vyplývajících všemi zaměstnanci a ostatními participujícími osobami. S ohledem na maximální zabezpečení informací je prováděno periodické, dokumentované monitorování a vyhodnocování bezpečnostních rizik a incidentů. Je zajišťováno neustálé zlepšování bezpečnosti informací (tj. zabezpečení včasné dostupnosti informací, zamezení jejich modifikace, zneužití a ztráty) v souladu s obecně závaznými právními a interními předpisy a smluvními požadavky a s požadavky systému řízení ve smyslu ustanovení jednotlivých prvků normy ISO/IEC 27001:2014 (dále jen ISO 27001) a TISAX.

Část první
Systém řízení bezpečnosti informací
Čl. I
Úvod

1. Tato politika stanovuje základní rámec systému bezpečnosti informací a určuje základní odpovědnosti za udržování a rozvoj tohoto systému ve společnosti.
2. Informací se rozumí jakýkoli údaj nebo soubor údajů o věcech, lidech a činnostech, které jsou získávány, zpracovávány, uchovávány a poskytovány libovolnou formou (písemnou, ústní nebo elektronickou). Pro potřeby zpracování jsou informace členěny (klasifikovány) do skupin. Popis jednotlivých skupin informací stanoví statutární vedoucí organizace vnitřním předpisem.
3. Bezpečnosti informací se rozumí zachování důvěrnosti, integrity a dostupnosti informací, jakož i zachování dalších vlastností informací, jako je jejich autentičnost, nepopiratelnost a spolehlivost.
4. Systémem řízení bezpečnosti informací se rozumí činnost organizace zaměřená na ustavení, zavádění, provoz, monitorování, přezkoumání, udržování a zlepšování bezpečnosti informací.
5. Bezpečnostním incidentem se rozumí stav informačních aktiv ukazující na možné porušení Základní politiky bezpečnosti informací nebo na selhání bezpečnostních opatření, u kterého existuje vysoká pravděpodobnost ohrožení činností organizace nebo bezpečnosti informací.
6. Rozsah systému řízení bezpečnosti informací je určen v čl. V této politiky.
7. Za ustavení, zavedení, provoz, monitorování, udržování a zlepšování systému řízení bezpečnosti informací odpovídají vedoucí zaměstnanci.

Čl. II
Rozsah a kontext ISMS

1. Systém řízení bezpečnosti informací je implementován v rozsahu požadavků ISO 27001 a normy TISAX, vyjma části spojené s vývojem.
2. Systém řízení bezpečnosti informací je platný pro všechna pracoviště, pracovníky a spolupracující osoby společnosti.
3. Z hlediska činnosti je systém zabezpečení informací zaveden pro:
   - Všechny činnosti a aktivity spojené se zpracováním osobních údajů,
   - Všechny činnosti a postupy ovlivňující bezpečnost informací společnosti, včetně informační bezpečnosti dat a informací klientů a dalších třetích stran.
4. Společnost při své podnikatelské aktivitě široce aplikuje postupy automatizace a elektronického zpracování dat, kdy mimo informací přístupných široké veřejnosti, jsou zpracovávány také

strategické informace, obchodní tajemství a informace podléhající režimu zákona o ochraně osobních údajů, resp. příslušné direktivy EU a navazujících předpisů.

5. Způsob zpracování a ukládání informací je definován souborem cílů a pravidel (dokumentované postupy jako další úroveň Základní politiky bezpečnosti informací), které jsou vedením podporovány a sdělovány všem zaměstnancům.
6. Z hlediska zabezpečení informací jsou vnímány požadavky zainteresovaných stran, tj. jejich potřeby a očekávání (ať už byly vyhlášeny, všeobecně se předpokládají nebo jsou závazné):
   a) Osoby – diskrétnost, ochrana osobních údajů a omezení přístupu k informacím na nezbytně nutnou míru;
   b) Zaměstnanci - ochrana osobních údajů, včasná dostupnost informací související se zaměstnáním, zachování identity při zpracování informací;
   c) Zákazníci – ochrana zákaznických dat a ochrana obchodního tajemství
   d) Dodavatelé – ochrana autorských práv, plnění smluvních závazků a ochrana obchodního tajemství;
   e) Orgány veřejné správy – včasná a zabezpečená komunikace;
   f) Zájmové skupiny – včasná a zabezpečená komunikace;
7. Náklady na zajištění bezpečnosti informací musí být souměřitelné s hodnotou možných dopadů a jejich výše musí být přiměřená.

Čl. III
Odpovědnost vedoucích zaměstnanců

Vedoucí zaměstnanci v rámci řízení systému bezpečnosti informací odpovídají zejména za:

- provádění pravidelného monitorování a vyhodnocování bezpečnostních rizik a navrhování odpovídajících (efektivních) opatření vedoucích k omezení jejich vlivu;
- propagaci významu dodržování zásad bezpečnosti informací ve vztahu k podřízeným zaměstnancům;
- integraci požadavků na řízení bezpečnosti informací vyplývajících z právních předpisů, ze smluvních ujednání nebo z dalších závazných aktů do procesů a činnosti organizace;
- pravidelné roční přezkoumávání funkčnosti systému řízení bezpečnosti informací a souladu zpracování informací v oblasti své působnosti s příslušnými bezpečnostními politikami, normami a směrnicemi organizace. Pokud vedoucí pracovník při přezkoumání nalezne jakýkoli nesoulad, identifikuje příčinu nesouladu, vyhodnotí potřebu kroků vedoucích k souladu, implementuje příslušná nápravná opatření a následně ověří jejich efektivnost. Výsledky přezkoumání a nápravných opatření zaznamená a předá jako podklad pro přezkoumání ISMS vedením BM (viz článek XIII.).;
- uplatnění požadavků na dostatečné finanční zdroje pro realizaci systému řízení bezpečnosti informací, zejména pro realizaci opatření navržených ke snižování rizik;
- stanovování a schvalování cílů potřebných pro zlepšení bezpečnosti informací;
- koordinaci bezpečnostních opatření v rámci společnosti;

Čl. IV
Povinnosti zaměstnanců a spolupracujících osob

Zaměstnanci a spolupracující osoby společnosti jsou povinni zejména:

- používat pouze informační prostředky nezbytné k plnění jejich pracovních povinností;
- nakládat s informačními prostředky nezbytnými k plnění pracovních povinností tak, aby byla zachována bezpečnost informací a nedocházelo k bezpečnostním incidentům;
- v případě vzniku bezpečnostního incidentu informovat bez zbytečného odkladu svého přímého nadřízeného nebo jeho zástupce a učinit všechna opatření k minimalizaci následků takového incidentu;
- dodržovat základní zásady práce s informacemi a jejich zabezpečení.

Čl. V
Základní zásady práce s informacemi a způsob jejich zabezpečení

1. Systém řízení bezpečnosti informací je vystavěn na následujících zásadách:
   - zajištění ochrany osobních údajů v souladu s platnou legislativou,
   - vytváření a prosazování systému řízeného přístupu k informacím,
   - provádění stálé identifikace bezpečnostních incidentů a přijímání účinných opatření pro zlepšování bezpečnosti informací,
   - zajišťování systematického vzdělávání a zvyšování kvalifikace zaměstnanců v oblasti bezpečnosti informací,
   - zpracovávání opatření pro zachování kontinuity pro případy závažného výpadku v oblasti informací, pravidelné přezkušování a ověřování těchto opatření,
   - zabezpečování informačních systémů, internetu, elektronické pošty a dalších způsobů výměny informací přístupných veřejnosti,
   - zabezpečování systému fyzického přístupu do prostor,
   - nepřetržité zajišťování dostupnosti, spolehlivosti a integrity dat,
   - prosazování politiky bezpečného pracoviště, tzn. dodržování zásady čistého stolu, prázdné obrazovky a odpadkového koše bez zabezpečených informací,
   - dodržování bezpečnostních pravidel pro přenosná počítačová zařízení a jiné nosiče informací,
   - zajišťování spolehlivé kontroly celé interní sítě proti působení zlomyslného softwaru, spolehlivé chránění a zálohování informací,
   - sdělování a výměnu informací s třetí stranou lze provádět pouze na základě zákona, nebo na základě smlouvy uzavřené v písemné formě.
2. Konkrétní povinnosti vyplývající z uplatňování zásad stanovených v odstavci 1 tohoto článku stanoví vedení společnosti vnitřním předpisem.

Část druhá
Interní organizace

Čl. VI
Odpovědnost a koordinace ISMS

1. Pro zajištění implementace, rozvíjení a neustálého zlepšování systému bezpečnosti informací se zřizují tyto role a orgány:
   a. Bezpečnostní fórum (BF)
   b. Bezpečnostní manažer pro ISMS (BM)

2. Obsazení orgánů provede vedení společnosti jmenováním formou určovací listiny pro stanovení hlavních odpovědností za systém bezpečnosti informací (a., b.). Povinnosti a odpovědnosti jednotlivých rolí jsou určeny v interních jmenovacích dekretech.

Čl. X
Informační aktiva

Pro účely analýzy rizik jsou vedeny přehledy všech skupin informačních aktiv, které pravidelně projednává a schvaluje BF.

Odpovědnost za ostatní informační aktiva (SW, HW) je definována interními předpisy společnosti. Manažerem agendy, kterou využívá jeden odbor, je vždy vedoucí tohoto odboru. Manažera agendy, kterou využívá více odborů, jmenuje na návrh BM vedení společnosti.

Čl. XI
Monitorování, měření, analýza a hodnocení ISMS

1. BM stanovuje roční cíle pro sledované indikátory (viz odst. 2) v oblasti ISMS.
2. BM ISMS zabezpečuje sledování a vyhodnocování hlavních indikátorů systému řízení bezpečnosti informací v těchto oblastech:

a) Rizika
- Jednotlivá rizika jsou identifikována v samostatném dokumentu – Analýza rizik, kde k nim jsou přiřazeny hodnoty, dle pravděpodobnosti vzniku a dopadu na společnost.

Účinnost přijatých opatření
Jednotlivá opatření na zvládání rizik jsou považována za účinné, pokud:
- pozitivně ovlivní související zranitelnosti nebo
- podporuje účinnost jiných opatření (např. implementace organizačních opatření na podporu zavedených technických opatření a naopak) nebo
- sníží hodnotu alespoň jednoho souvisejícího rizika.

b) Incidenty, nápravná a preventivní opatření
- poměr počtu incidentů a přijatých nápravných opatření v plánovaném termínu;

Čl. XII
Audity a kontrola IS*M*S

1. Systém řízení bezpečnosti informací podléhá pravidelným auditům prováděným autorizovanou osobou. Za včasnost a úplnost provádění těchto auditů odpovídá BM.
2. Systém řízení bezpečnosti informací dále podléhá interním auditům. Interní audity všech prvků budou plánovány a prováděny vždy během jednoho kalendářního roku. Během tohoto období bude prověřeno, zda realizovaná opatření splňují požadavky normy ISO 27001/TISAX, odpovídají legislativě pro ochranu osobních údajů, zákonným a jiným regulativním požadavkům, zda tato opatření fungují efektivně a podle očekávání a vyhovují identifikovaným požadavkům. Program auditů bude stanoven s ohledem na stav a význam procesů a výsledky minulých auditů. Odpovědnost za plánování, realizaci, hlášení výsledků a udržování záznamů má Auditor informační bezpečnosti. Navržená opatření zahrnují případnou nápravu i nápravná opatření. Kontrolu způsobu a rozsahu provádění auditů ISMS provádí statuární vedoucí organizace 1x za rok na základě vlastního plánu.
   Vedoucí zaměstnanci jsou odpovědni za odstraňování nedostatků a jejich příčin. Auditoři nesmí auditovat vlastní práci a musí být pravidelně proškolováni.
3. V rámci systému řízení bezpečnosti informací probíhají kontroly a monitoring důležitých procesů určených Plánem monitoringu a kontrol, který vede BM. Tato kontrola také zahrnuje monitoring činnosti zaměstnanců s cílem bezpečného a efektivního využití výpočetních prostředků. Při provádění monitoringu musí být ošetřena práva zaměstnanců na ochranu soukromí.

Čl. XIII
Přezkoumání systému řízení bezpečnosti informací vedením organizace

1. Přezkoumání systému řízení bezpečnosti informací provádí BM po projednání této zprávy v BF a jejím připomínkováním. Cílem přezkoumání je zajistit, že je bezpečnost informací implementována a provozována v souladu s politikami a postupy organizace a že je vhodná, přiměřená a efektivní pro dosahování politiky a cílů společnosti. Přezkoumání vždy zahrnuje posouzení příležitostí pro zlepšování a potřebu změn.
2. Přezkoumání se provádí 1x za kalendářní rok, nebo při významné změně interních nebo externích podmínek.
3. Podklady pro sestavení zprávy pro přezkoumání systému předají BM vedoucí zaměstnanci. Podkladem pro sestavení zprávy jsou vždy informace o:
   - přiměřenosti a aktuálnosti této politiky, revizi všech souvisejících organizačně a řídících dokumentů pro oblast ISMS,

- stavu opatření (preventivních opatření a opatření k nápravě) z předchozích přezkoumání vedením organizace,
- změnách v externím a interním aspektu, které jsou relevantní pro ISMS,
- zpětná vazba na výkonnost (měření účinnosti) ISMS, včetně trendů ohledně:
  - neshod a nápravných opatření,
  - výsledků monitorování a měření,
  - výsledků auditů a jiných přezkoumání, zejména vyhodnocení Plánu monitoringu a kontrol IT,
  - naplnění cílů ISMS,
- zpětných vazbách od zainteresovaných stran, tj. subjektů, které mohou ovlivnit bezpečnost informací nebo jejichž informace jsou zpracovávány (např. kontrolní orgány, občané dodavatelé),
- výsledcích posuzování rizik a stavu plánu pro ošetření rizika, hodnocení rizik, incidentů a neshod,
- příležitostech pro neustálé zlepšování, zejména:
  - činnosti, které následovaly po předchozím přezkoumání vedením,
  - techniky, produkty nebo postupy, které by mohly zvýšit efektivitu,
  - aktiva, zranitelnosti, nebo hrozby, jimž nebyla v rámci předchozích přezkoumání rizik věnována náležitá pozornost, nebo u kterých došlo ke změnám,
  - změny, které by mohly ovlivnit činnost organizace,

4. Součástí zprávy musí být návrhy na opatření k jednotlivým bodům zprávy, zejména rozhodnutí vztahující se k
   - příležitostem neustálého zlepšování
   - jakýmkoli potřebám pro změny v ISMS.
5. Zprávy jsou uchovávány jako důkazy o výsledcích přezkoumání vedením organizace po dobu 10 let.

Část třetí
Závěrečná ustanovení
Čl. XIV

Tato politika byla schválena vedením společnosti, níže uvedeným podpisem a nabývá účinnost datem podpisu.

V Opavě dne 2.1.2023

Ing. Lukáš Grebeníček
ředitel společnosti