Závazek vedení

Vedení RAMA Bohemia s.r.o. se zavazuje podporovat zavedení a provoz ISMS a to: stanovením Bezpečnostní politiky informací organizace, stanovením cílů ISMS a plánu na jejich dosažení, stanovením rolí, povinností a odpovědností v oblasti bezpečnosti informací, propagací významu plnění cílů bezpečnosti v rámci organizace, zajištěním potřebných zdrojů, stanovením kritérií pro akceptaci rizik a akceptovanou úroveň rizika, zajištěním provádění interních auditů ISMS a prováděním přezkoumání ISMS vedením organizace.

Cíle a význam bezpečnosti informací v organizaci

Obecným cílem ISMS je zajistit spolehlivost a bezpečnost informačních technologií provozovaných pro podporu činností organizace a manipulaci informací v listinné formě. **Hlavním cílem** je zajistit bezpečnost citlivých informací z pozice dodavatele a poskytovatele služeb v automobilovém průmyslu (v některých případech je certifikace TISAX považována za závaznou podmínku smlouvy s automobilovými výrobci).

Bezpečnostní strategie organizace

Systém řízení bezpečnosti informací je zaveden v souladu s certifikací TISAX
Důležitým aspektem je vybudování ISMS, který vyžaduje především:
- Zavedení základních procesů ISMS,
- Systém řízení rizik s následným výběrem opatření,
- Interní kontrolní systém a pravidelné hodnocení stavu.

Základními oblastmi ISMS jsou:

1. Politiky a organizace bezpečnosti	5. Bezpečnost IT / kybernetická bezpečnost
2. Lidské zdroje	6 Dodavatelské vztahy
3. Fyzická bezpečnost a kontinuita činností	7. Shoda
4. Správa identit a řízení přístupu	

Hodnocení rizik a požadavky na bezpečnost informací

Hodnocení aktiv se provádí z hlediska požadavků na jejich důvěrnost, dostupnost a integritu. Po určení aktiv se identifikují jejich zranitelnosti a hrozby a následuje jejich ohodnocení. Posouzení rizik je prováděno na základě identifikace, analýzy a hodnocení rizik a má za cíl určit možné hrozby, zranitelnosti a rizika hodnoceného systému, odhadnout ztráty, které mohou vzniknout působením hrozeb na informační aktiva zařazená do ISMS organizace. K pokrytí zjištěných rizik, předcházení nebo snížení nežádoucích následků a k dosažení neustálého zlepšování se přijímají bezpečnostní opatření (Prohlášení o aplikovatelnosti, Plán zvládání rizik). Posouzení rizik a hodnocení aktiv se provádí pravidelně jednou za tři roky nebo v případě větších změn v posuzované oblasti.

Základní definice odpovědností

Vedení organizace definuje funkce, kterým jsou přiděleny příslušné role, odpovědnosti a pravomoci.

Bezpečnostní manažer – odpovídá vedení organizace, realizuje bezpečnostní zásady bezpečnostní politiky informací organizace a navrhuje její změny, sleduje dodržování bezpečnostních opatření a realizaci jejich změn, zabezpečuje hodnocení rizik, řešení bezpečnostních incidentů a zvyšování bezpečnostního povědomí zaměstnanců organizace.
Garant aktiva – bezpečnostní role odpovědná za zajištění rozvoje, použití a bezpečnost aktiva.
Auditor ISMS – zaměstnanec, který je určen jako interní auditor ISMS organizace.

Problematika bezpečnosti informací je pravidelně projednávána na jednání vedení, kterého se účastní bezpečnostní manažer organizace a je prováděno minimálně 1x za půl roku či v případě naléhavé potřeby.

Požadavek na školení a vzdělávání

Společnost dohlíží na to, aby zaměstnanci, kterých se týkají povinnosti definované v ISMS, byly odborně způsobilí k výkonu požadovaných úkolů. Způsobilost je udržována školením či vzděláváním dle profesí a v intervalech stanovených v platných předpisech.

Interní audit

K zajištění ochrany provozovaných informačních systémů a systému ISMS je prováděn pravidelný audit bezpečnosti informací. Auditní požadavky a činnosti zahrnující kontrolu ISMS organizace jsou plánovány auditorem ISMS a schváleny vedením organizace v periodě minimálně 1 x ročně.

Pravidelné přezkoumání

Přezkoumání systému managementu bezpečnosti informací se provádí s cílem zajistit účelnost, adekvátnost a efektivnost provozovaného ISMS v organizaci. Přezkoumání ISMS zároveň uvádí možnosti zlepšení a návrh změn v provozovaném ISMS. Interval přezkoumání ISMS je v RAMA Bohemia s.r.o., stanoven na 1x ročně.

Uvedení důsledků v případě nedodržení politiky

Všichni zaměstnanci jsou seznámeni se skutečností, že nedodržení bezpečnostních zásad může být kvalifikováno jako porušení povinností zaměstnance a v některých případech i jako přestupek nebo trestný čin.

Způsob revize

Politiky pro bezpečnost informací jsou k dispozici na www.rama-cz.com pro všechny zaměstnance a externí partnery. Revize všech bezpečnostních politik je prováděna jejich vlastníkem minimálně 1x ročně nebo při změně jakékoliv bezpečnostní politiky. Datum revize je vždy zaznamenáno v příslušné bezpečnostní politice.

Navazující dokumentace

Na BPI RAMA Bohemia s.r.o., navazuje dokumentace ISMS rozpracovávající opatření pro oblasti bezpečnosti informací. Tyto dokumenty obsahují konkrétní odpovědnosti za realizaci procesů a činností bezpečnosti informací RAMA Bohemia s.r.o.
Hierarchie dokumentace ISMS RAMA Bohemia s.r.o., je následující:

1. Bezpečnostní politika informací (tato politika),
2. Směrnice bezpečnosti informací a Uživatelská bezpečnostní směrnice,
3. Záznamy pro podporu ISMS (zejména dokumentace hodnocení rizik, dokumentace bezpečnostních zón, dokumentace spojená s dodavateli, evidence bezpečnostních incidentů, plán kontinuity činností, dokumentace interních auditů ISMS, evidence neshod a pravidelní přezkoumání stavu bezpečnosti informací).

Řízení dokumentace ISMS RAMA Bohemia s.r.o., se řídí směrnicí QUA-S-DM-005_Směrnice řízení dokumentace.

V Obříství

Dne 2.3.2022

Rastislav Proks

.....

Majitel firmy – Proks Rastislav

RAMA BOHEMIA, a.s.
Londýnská 309/81, Praha 2
Provozovna: Obříství 231, 277 42
tel: 326 538 001, fax: 326 538 000
DIČ: CZ49241591