GLOBAL ASSISTANCE a.s., Praha 8, Dopraváků 749/3, IČO 27181898

Politika informační bezpečnosti

Úvodní ustanovení

Účelem této politiky je stanovení a definování pravidel informační bezpečnosti ve společnosti GLOBAL ASSISTANCE a.s. v návaznosti na Strategii informační bezpečnosti. Tento předpis je určen pro vnitřní potřebu organizace a je závazný pro všechny její zaměstnance.

Definice informační bezpečnosti a ISMS

Informační bezpečnosti je dosaženo zavedením vhodného souboru opatření, včetně politik, pravidel, procesů, postupů, organizačních struktur a funkcí softwaru a hardwaru. Aby organizace splnila své specifické cíle bezpečnosti a činnosti, má tato opatření definovat, zavést, monitorovat, přezkoumávat a v případě potřeby zlepšovat.

Systém managementu informační bezpečnosti (dále také „ISMS“), jako je systém specifikovaný v ISO/IEC 27001, zaujímá celkový, koordinovaný pohled na rizika informační bezpečnosti organizace s cílem určit a zavést komplexní soubor opatření informační bezpečnosti v celkovém rámci koherentního systému managementu.

Cíl informační bezpečnosti

Hlavním cílem ISMS ve společnosti GLOBAL ASSISTANCE a.s. je ochrana zpracovávaných informací s důrazem na zajištění jejich důvěrnosti a integrity při zachování jejich potřebné dostupnosti a ochrany proti náhodnému nebo cílenému narušení.

V souladu s hlavním cílem ISMS společnost GLOBAL ASSISTANCE a.s. dále **deklaruje snahu plnit následující cíle**:

1. Dodržovat všechny právní a vnitřní předpisy týkající se ochrany dat a informací s důrazem na zajištění informační bezpečnosti.
2. Integrovat procesy ISMS do procesů společnosti.
3. Zavést a udržovat ISMS a bezpečnostní opatření efektivně tak, aby bylo dosaženo nejvyšší možné míry bezpečnosti bez jakéhokoli omezení poskytování služeb společnosti.
4. Zajistit efektivní výběr bezpečnostních opatření na ochranu dat a informací na základě pravidelného provádění hodnocení rizik.
5. Zajistit odpovědnost za jednotlivé oblasti informační bezpečnosti s využitím systému bezpečnostních funkcí a rolí.
6. Ve vztahu k zaměstnancům společnosti GLOBAL ASSISTANCE a.s.:

a. komunikovat s nimi potřebu zajištění informační bezpečnosti s důrazem na pochopení jejich podílu,
b. zajistit znalost bezpečnostních postupů zaměstnanců s využitím komplexního systému bezpečnostního vzdělávání,
c. zabezpečit odpovídající kvalifikaci zaměstnanců pověřených výkonem bezpečnostních rolí formou pravidelných specializovaných školení v oblasti informační bezpečnosti.

7. Uplatňovat relevantní bezpečnostní kritéria při výběru dodavatelů výrobků, služeb a při uzavírání obchodních vztahů k zajištění nejvyšší možné míry bezpečnosti dodávaných služeb.
8. Zajistit pravidelné přezkoumání stavu informační bezpečnosti ve společnosti GLOBAL ASSISTANCE a.s. a prosazovat neustálé zlepšování systému managementu informační bezpečnosti.

V návaznosti na výše uvedené cíle jsou stanoveny dílčí cíle na kalendářní rok, které vypracuje Manažer informační bezpečnosti (dále také „MIB“) a jež dále schvaluje Skupina informační bezpečnosti (dále také „SIB“) v rámci pravidelného ročního přezkoumání ISMS.

Zásady informační bezpečnosti

Zásady informační bezpečnosti tvoří následující oblasti opatření:

1. Organizační opatření,
2. Opatření v oblasti lidských zdrojů,
3. Opatření fyzické bezpečnosti,
4. Technologická opatření.

Konkrétní opatření ve výše uvedených oblastech jsou přijímána na základě hodnocení aktiv a rizik.

Opatření jsou rozpracována v bezpečnostní dokumentaci společnosti GLOBAL ASSISTANCE a.s.

Závazek vedení splnit platné požadavky týkající se informační bezpečnosti

Vedení GLOBAL ASSISTANCE a.s. se zavazuje podporovat zavedení a provoz systému managementu informační bezpečnosti (dále jen „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.

Závazek k neustálému zlepšování ISMS

Společnost GLOBAL ASSISTANCE a.s. se zavazuje pravidelně zlepšovat provozovaný systém managementu informační bezpečnosti na základě pravidelného hodnocení jeho stavu.

Hodnocení stavu probíhá formou přezkoumání ISMS. Přezkoumání systému managementu bezpečnosti informací se provádí s cílem zajistit účelnost, adekvátnost a efektivnost provozovaného ISMS ve společnosti. Přezkoumání ISMS zároveň uvádí možnosti zlepšení a

návrh změn v provozovaném ISMS. Interval přezkoumání ISMS je ve společnosti GLOBAL ASSISTANCE a.s. stanoven na jednou ročně.

Přezkoumání ISMS zpracovává MIB, předkládá je k projednání SIB a schvaluje je vedení společnosti GLOBAL ASSISTANCE a.s.

Obsah a způsob provedení přezkoumání ISMS je uveden ve Směrnici informační bezpečnosti.

Přidělení odpovědností za ISMS definovaným rolím

Vedení organizace definuje funkce, kterým jsou přiděleny příslušné role, odpovědnosti a pravomoci pro řízení bezpečnosti informací.

Skupina informační bezpečnosti (SIB) – je tvořena osobami s příslušnými pravomocemi a odbornou způsobilostí pro celkové řízení a rozvoj ISMS a osobami významně se podílejícími na řízení a koordinaci činností spojených s bezpečností informací. Členem SIB musí být vždy alespoň jeden zástupce vrcholového vedení společnosti nebo jím pověřená osoba a Manažer informační bezpečnosti.

Manažer informační bezpečnosti (MIB) – odpovídá vedení společnosti. Realizuje bezpečnostní zásady politiky informační bezpečnosti společnosti 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 – je bezpečnostní role odpovědná za definici požadavků na rozvoj, použití a bezpečnost primárního nebo podpůrného aktiva.

Garant rizika – je role odpovědná za správu relevantních identifikovaných rizik s důrazem na přijímání a schválení opatření k jejich pokrytí.

Auditor ISMS – je osoba nebo externí dodavatel, který je určen jako interní auditor systému managementu informační bezpečnosti společnosti.

Za jmenování rolí odpovídá vedení společnosti GLOBAL ASSISTANCE a.s.

Rozpracování odpovědností, nároky na jejich kompetence, zastupitelnost a neslučitelnost jsou vedeny ve Směrnici organizační bezpečnosti.

Posouzení rizik a požadavky na bezpečnost informací

Hodnocení aktiv se provádí z hlediska požadavků na jejich důvěrnost, dostupnost a integritu. Posouzení rizik je prováděno na základě identifikace, analýzy a hodnocení rizik. Má za cíl určit možné hrozby, zranitelnosti a rizika hodnoceného systému a odhadnout ztráty, které mohou vzniknout působením hrozeb na 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 ošetření rizik). Posuzování rizik a hodnocení aktiv se provádí pravidelně jednou za tři roky nebo v případě větších změn v posuzované oblasti.

Za organizaci hodnocení aktiv a rizik odpovídá MIB, za hodnocení jednotlivých aktiv jejich garanti. Hodnocení aktiv a rizik je dále rozpracováno v Metodice hodnocení aktiv a rizik.

Požadavek na školení a vzdělávání

Organizace dohlíží na to, aby zaměstnanci, kterých se týkají povinnosti definované v ISMS, byli odborně způsobilí k výkonu požadovaných úkolů. Způsobilost je udržována školením či vzděláváním dle rolí v intervalech stanovených v interních předpisech.

Zaměstnanci jsou povinni absolvovat vstupní školení k informační bezpečnosti a pravidelná roční školení ISMS. Mimořádná školení se provádí v případě větší změny, při nasazení nových informačních systémů a při reakci na závažné bezpečnosti incidenty.

Za organizaci školení v oblasti informační bezpečnosti odpovídá personální oddělení.

Rozpracování školení a vzdělávání je uvedeno v Programu zvyšování povědomí o informační bezpečnosti.

Interní audit

K zajištění systému ISMS je prováděn pravidelný audit informační bezpečnosti. Auditní požadavky a činnosti zahrnující kontrolu ISMS organizace jsou plánovány Auditorem ISMS a schváleny poradou vedení v periodě minimálně jednou ročně.

Za realizaci auditu ISMS odpovídá Auditor ISMS.

Provádění auditu ISMS včetně jeho hodnocení je rozpracováno v Organizační směrnici ISMS a ve Směrnici Interní audity.

Postupy pro zpracování osvobození a výjimek

V případě, že nelze dodržet pravidla definovaná bezpečnostní dokumentací společnosti, může být udělena tzv. výjimka z bezpečnostních pravidel. Cílem zavedení výjimek je zajistit řízené schvalování a evidování nesouladu stavu informační bezpečnosti společnosti s definovanými bezpečnostními pravidly.

Požadavek na výjimku z bezpečnostních pravidel je předkládán k posouzení a schválení MIB.

Evidence výjimek musí obsahovat rozsah výjimky, bezpečnostní pravidlo, které se neuplatňuje, odůvodnění výjimky, navrhovatele, schvalovatele a status (aktivní/ukončená). Výjimky eviduje MIB a pravidelně je reviduje (jednou ročně). O schválených výjimkách MIB informuje SIB.

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.

Schválení a způsob revize politiky

Politika informační bezpečnosti a navazující bezpečnostní dokumentace jsou k dispozici v knihovně Směrnice pro všechny zaměstnance a pro externí partnery ve smluvní dokumentaci a na extranetu. Revize bezpečnostní dokumentace je prováděna jejich vlastníkem minimálně 1x ročně nebo při změně jakékoliv bezpečnostní politiky. Datum revize je vždy zaznamenáno v příslušném dokumentu.

Vrcholové vedení schvaluje veškeré změny politiky informační bezpečnosti.

Navazující dokumentace

Na Bezpečnostní politiku informací společnosti GLOBAL ASSISTANCE a.s. navazuje dokumentace ISMS rozpracovávající opatření pro oblasti informační bezpečnosti. Tyto dokumenty vymezují konkrétní odpovědnosti za realizaci procesů a činností ISMS společnosti GLOBAL ASSISTANCE a.s.

Hierarchie dokumentace ISMS společnosti GLOBAL ASSISTANCE a.s. je následující:

1. Bezpečnostní politika informací (tato politika),
2. Organizační směrnice ISMS,
3. Směrnice bezpečnosti IT,
4. Bezpečnostní uživatelská příručka,
5. 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 pravidelné přezkoumání stavu bezpečnosti informací).

Řízení dokumentace ISMS společnosti GLOBAL ASSISTANCE a.s. se řídí podle interní Směrnice Řízení dokumentace a záznamů.

19.11.2024