Datum vydání: 24. 4. 2023
Účinnost: 24. 4. 2023
Závaznost: FSI VUT
Nahrazuje: -
Doplňuje: -
Vydává: děkan FSI VUT
Počet stran: 5
Počet příloh: -
Rozdělovník: děkan**,** proděkani, tajemník, ředitelé ústavů, ředitelé a vedoucí specializovaných pracovišť, vedoucí oddělení děkanátu, tajemníci ústavů

ROZHODNUTÍ DĚKANA Č. 2/2023

POLITIKA BEZPEČNOSTI INFORMACÍ

FAKULTY STROJNÍHO INŽENÝRSTVÍ

VYSOKÉHO UČENÍ TECHNICKÉHO V BRNĚ

Vedení Fakulty strojního inženýrství Vysokého učení technického v Brně (dále jen „fakulta“) deklaruje, že dobrovolně přijímá a zavazuje se dodržovat níže uvedená pravidla a opatření s cílem zajistit, aby chování fakulty a všech jejích součástí, zaměstnanců, orgánů a jejich členů i dalších spolupracujících osob (zejména externí konzultanti a poradci včetně jejich zaměstnanců), které ve věcech fakulty jednají jménem nebo ve prospěch VUT či v jeho zastoupení, bylo v plném souladu s požadavky ochrany a bezpečnosti informací dle mezinárodní normy ČSN EN ISO/IEC 27001 Informační technologie - Bezpečnostní techniky - Systémy řízení bezpečnosti informací - Požadavky (dále jen „mezinárodní norma ISO/IEC 27001“) a požadavků TISAX.

Fakulta prohlašuje, že:

1) Hlavním cílem je zajištění bezpečnosti informací pomocí přiměřených a odpovídajících opatření, která budou chránit informační aktiva tak, aby byla poskytnuta odpovídající míra jistoty.

2) Tento cíl je naplňován vybudováním, zavedením, provozováním, kontrolováním, údržbou, průběžnou evaluací a neustálým zlepšováním dokumentovaného systému řízení bezpečnosti informací v kontextu aktivit a rizik fakulty.

3) Pojmem bezpečnost informací rozumíme proces zajišťování ochrany informací na potřebné úrovni z hlediska jejich důvěrnosti, integrity a dostupnosti.

4) Základními zdroji pro řízení bezpečnosti informací jsou právní předpisy, standardy, normy a doporučení, které musí být v procesu řízení bezpečnosti informací respektovány.

5) Pro zajištění všech požadovaných úkolů, případně plnění legislativních požadavků, jsou vytvářeny, zpracovávány a udržovány informace různého charakteru, které vyžadují adekvátní úroveň ochrany.

6) Fakulta naplňuje jednotlivé bezpečnostní cíle pomocí adekvátních opatření, určených v rámci procesu řízení rizik bezpečnosti informací v oblastech organizace bezpečnosti, klasifikace informací, personální a fyzické bezpečnosti, bezpečnosti prostředí, bezpečnosti řízení komunikací a provozu, řízení bezpečnosti přístupu, bezpečnosti vývoje a údržby systémů, řízení kontinuity provozu, a to v souladu s legislativními požadavky tak, jak je vymezeno v Příručce implementace procesů informační bezpečnosti.

7) Tímto rozhodnutím se vedení fakulty přihlašuje k implementaci procesů informační bezpečnosti, včetně nezbytné podpory finanční, materiální a personální.

Úvodní ustanovení

1. Tato Politika bezpečnosti informací zavádějící pravidla v oblasti systému řízení bezpečnosti informací (dále jen „Pravidla“) je základním strategickým dokumentem zajišťujícím rámec informační bezpečnosti fakulty.
2. Pravidla se vztahují na veškeré informační systémy a veškeré informace, které jsou v rámci fakulty zpracovávány (dále jen „informační aktiva“). Cílem těchto Pravidel je zejména:
    a) určit cíle informační bezpečnosti,
    b) stanovit hlavní zásady informační bezpečnosti,
    c) vymezit bezpečnostní potřeby fakulty,
    d) specifikovat dokumentaci informační bezpečnosti,
    e) vytvořit systém řízení bezpečnosti informací, tj. definovat práva a povinnosti ve vztahu k řízení bezpečnosti informací,
    f) zavést bezpečnostní opatření na základě bezpečnostních potřeb a výsledků hodnocení rizik.
3. Vedení fakulty se tímto dokumentem hlásí k naplňování a dodržování všech zásad informační bezpečnosti, které jsou definovány v tomto a ostatních dokumentech bezpečnostní politiky fakulty.

Cíle Politiky bezpečnosti informací

1. Zajištění požadované úrovně ochrany z hlediska dostupnosti, důvěrnosti a integrity informačních aktiv fakulty. Veškeré významné uživatelské operace s informačními aktivy jsou jednoznačně identifikovány, bezpečně zaznamenávány a následně vyhodnocovány.
2. Schopnost detekovat kybernetické bezpečnostní incidenty, a to včetně identifikace původce bezpečnostního incidentu, způsobu narušení bezpečnosti, dopadů a přijmutí příslušných reaktivních bezpečnostních opatření.
3. Zavedení a řízení bezpečnostních opatření a udržování aktualizované bezpečnostní dokumentace.
4. Aplikovat procesní rámec řízení informační bezpečnosti na fakultě.

Hlavní zásady Politiky bezpečnosti informací

1. Zajištěním bezpečnosti informací se pro účely této politiky rozumí zachování důvěrnosti, integrity a dostupnosti informací a s nimi spojené priority, typicky autentičnost, odpovědnost, nepopiratelnost a spolehlivost.
2. Informační bezpečnost je na fakultě chápána jako komplexní proces ochrany informačních aktiv tvořený opatřeními personální bezpečnosti, fyzické bezpečnosti, bezpečnosti informačních technologií, plánováním kontinuity činností a zajištěním souladu s požadavky obecně závazných právních předpisů a jiných závazných norem v oblasti bezpečnosti informací.
3. Fakulta má jasně stanovena pravidla, kompetence a odpovědnosti v oblasti informační bezpečnosti a každý zaměstnanec je s nimi seznámen.

Bezpečnostní potřeby

1. Bezpečnostní potřeby pro jednotlivá informační aktiva vychází z jejich kategorizace na základě předchozího ohodnocení a dále z klasifikace zpracovávaných informací.

Systém Politiky bezpečnosti informací

1. Celkový systém Politiky bezpečnosti informací je vypracován v souladu:
    a) s mezinárodní normou ISO/IEC 27001,
    b) se zákonem č. 110/2019 Sb., o zpracování osobních údajů,
    c) s Nařízením Evropského parlamentu a Rady EU 2016/679 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto

údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů) – označované zkratkou GDPR,

d) požadavky TISAX,

e) ostatními požadavky danými obecně závaznými právními předpisy,

f) úrovní rizik, která hrozí informačním aktivům fakulty,

g) potřebami fakulty v oblasti zpracování a ochrany informací.

2. Bezpečnostní politiku tvoří dokumenty tří úrovní:

   a) Politiky – začleňují bezpečnost informací do kontextu celkové bezpečnosti organizace a definují základní bezpečnostní principy,

   b) Směrnice – obsahují zpravidla popis realizace vybraných bezpečnostních prvků a bezpečnostních opatření pro konkrétní principy politiky a konkrétní standardy. Obsahují technické údaje popisující použitý software, hardware, použitá procedurální či organizační opatření a způsob jejich implementace.

   c) Pracovní a procesní postupy – definují pracovní postupy nezbytné pro dodržení bezpečnostních standardů.

   d) Záznamy – evidence provedených úkonů a záznam nastalých událostí.

Systém řízení bezpečnosti informací

1. Systém řízení bezpečnosti informací (dále jen „ISMS“) je založen na mezinárodní normě ISO/IEC 27001 a požadavcích TISAX.
2. K zajištění informační bezpečnosti na fakultě jsou definovány následující role:

   a) manažer kybernetické bezpečnosti,

   b) auditor kybernetické bezpečnosti,

   c) garant aktiva,

   d) výbor pro řízení informační bezpečnosti.

3. Na fakultě jsou formou auditu prováděna nezávislá přezkoumání:

   a) celkového ISMS,

   b) aktuálnosti a správnosti bezpečnostní dokumentace,

   c) aktuálního stavu bezpečnostních opatření,

   d) jiných prvků ISMS dle aktuální potřeby.

4. Na fakultě jsou řízena aktuální rizika informačních aktiv a k nim identifikovány relevantní hrozby, zranitelnosti a možné dopady.

Oblasti relevantní pro rozsah bezpečnosti informací

1. Pro fakultu jsou definované hranice ISMS/TISAX v lokalitě Technická 2896/2, 616 69 Brno.
2. Implementace je aplikována pro činnosti spojené s výzkumem, vývojem a testováním v oblasti strojního inženýrství.
3. Pro fakultu je definovaný rozsah ISMS níže uvedeným výčtem oblastí:
    1. politiky bezpečnosti informací,
    2. organizace bezpečnosti informací,
    3. bezpečnost lidských zdrojů,
    4. řízení informačních aktiv,
    5. řízení přístupu,
    6. kryptografie,
    7. fyzická bezpečnost a bezpečnost prostředí,
    8. bezpečnost provozu,
    9. bezpečnost komunikací,
    10. akvizice, vývoj a údržba systémů,
    11. vztahy s dodavateli a odběrateli resp. průmyslovými partnery,
    12. řízení incidentů bezpečnosti informací,
    13. aspekty řízení kontinuity provozu,
    14. soulad s požadavky právní úpravy a relevantních norem.

v. r.

doc. Ing. Jiří Hlinka, Ph.D.
děkan FSI VUT