POLITIKA SYSTÉMU MANAGEMENTU ZABEZPEČENÍ INFORMACÍ

(dále též „***Politika ISMS***“) společnosti **Sunsec, s.r.o.** (dále též „***Společnost***“) je přílohou směrnice ***Vedení ISMS*** (viz dokument **I5_Vedení_ISMS**), nahrazuje a ruší předchozí ***Politiku ISMS,*** ze dne 6. 11. 2019.

Vrcholové vedení Společnosti si je vědomo důležitosti zabezpečování informací, ustavuje proto Systém managementu zabezpečení informací ***Společnosti*** (dále též „***ISMS***“), zveřejňuje tuto politiku a zavazuje každého pracovníka ***Společnosti*** k odpovědnosti za její realizaci.

Realizujeme systém managementu zabezpečení informací

Vytvořili jsme, dokumentujeme, implementujeme, udržujeme a kontinuálně zlepšujeme systém ***ISMS***, procesy a činnosti.

Realizujeme systém ***ISMS*** s cílem:

- směřovat veškeré naše činnosti a procesy ke kontinuálnímu zlepšování systému ***ISMS***;
- implementovat principy managementu kvality a zvládání rizika, procesní a systémový přístup;
- stanovovat a udržovat odolnost systémů proti selhání, důvěrnost, dostupnost a integritu informací;
- zamezovat zneužití, prozrazení nebo zničení osobních údajů, informací a všech informačních aktiv;
- snižovat zranitelnost vůči externím i interním hrozbám;
- zajišťovat podporu, prostředí, komunikaci, povědomí, znalosti a dokumentaci;
- stanovovat kompetence, maximálně motivovat a zapojovat pracovníky do systému ***ISMS***;
- udržovat soulad s legislativními požadavky a požadavky normy ***ISO 27001, ISO 27002 a ISO 27003***;
- udržovat soulad se smluvními požadavky a očekáváními našich zákazníků.

Vrcholové vedení Společnosti podporuje ISMS

Vrcholové vedení ***Společnosti*** podporuje systém ***ISMS*** a zavazuje se:

- implementovat systém ***ISMS*** v rámci strategického směrování ***Společnosti***;
- podporovat a delegovat odpovědnost a nezávislost pro ***Auditory ISMS***, ***Výbor ISMS***, ***Manažera ISMS*** a ***Architekta ISMS***, kteří zajišťují odborné řízení ***ISMS***;
- zajišťovat dostupnost zdrojů a podmínky k dosahování výkonnosti ***ISMS***;
- zajišťovat podporu a implementaci všech procesů k dosahování efektivního ***ISMS***;
- poskytovat nezávislost pro interní audity a řešit zjištění interních auditorů;
- důsledně a efektivně realizovat opatření k rizikům, příležitostem a incidentům;
- podporovat kontinuální zlepšování ***ISMS*** a odolnost informačních systémů.

Zvyšování zabezpečení informací a odolnosti systémů

Realizujeme opatření ke zvyšování zabezpečení informací a odolnosti systémů:

- Zabezpečení informací zachovává důvěrnost, integritu a dostupnost informací aplikováním procesu řízení rizik a dává jistotu zainteresovaným stranám, že jsou rizika přiměřeně snížena;
- Implementujeme opatření k ošetření rizik bezpečnosti informací a testujeme účinnost a význam dopadů na fungování procesů ***Společnosti***;

- Stanovujeme rozsahu systému ***ISMS***, včetně struktury, hranic a vazeb ***ISMS***;
- Stanovujeme a prosazujeme prohlášení o politice systému ***ISMS***;
- Řídíme rizik:
    - stanovujeme přístupu organizace k hodnocení rizik,
    - identifikujeme rizika včetně určení aktiv a jejich vlastníků,
    - stanovujeme analýzu a vyhodnocení rizik,
    - identifikujeme a ohodnotíme varianty pro zvládání rizik,
    - vybíráme cíle opatření a jednotlivých opatření pro zvládání rizik,
    - vedení společnosti souhlasí s navrhovanými zbytkovými riziky a se zavedením ISMS;
- Řídíme systémově a uceleně managementu zabezpečení;
- Efektivně řídíme investice vkládané do systému ***ISMS***;
- Řídíme inventuru vlastních aktiv, jejich ocenění a klasifikaci;
- Řídíme odstranění nebo snížení rizik v oblasti informačních systémů;
- Zavádíme systémové a systematické přístupy při používání IT/IS;
- Zabezpečujeme pracovníky a vynucujeme technická opatření;
- Řídíme přístupy a práva v systému ***ISMS***;
- Řídíme a zabezpečujeme aktiva;
- Řídíme a zlepšujeme kryptografii;
- Řídíme fyzickou bezpečnost;
- Řídíme provoz a každodenní činnosti s cílem naplňovat cíle systému ***ISMS***;
- Zabezpečujeme sítě a komunikační prostředky;
- Řídíme vztahy a mlčenlivost dodavatelů;
- Řešíme incidenty a stanovujeme k nim opatření;
- Posilujeme kontinuitu a odolnost systémů a zařízení;
- Zvyšujeme povědomí a odpovědnosti pracovníků při práci s informacemi;
- Naplňujeme legislativní, normativní a smluvní požadavky;
- Udržujeme důvěryhodnost pro partnery;
- Trvale monitorujeme a zlepšujeme systém ***ISMS***;
- Udržujeme konkurenční výhoda, kultivace Image a firemní kultury;
- Zvyšujeme uvědomění pracovníků na všech úrovních a motivujeme je k provádění svých činností bezpečnostně vhodným způsobem;
- Vyzýváme naše subdodavatele a smluvní partnery k prokazování vyšší bezpečnostní uvědomělosti a formou řízené spolupráce působíme na zvyšování jejich povědomí k zabezpečování informací.

V Praze, dne 30. dubna 2024

V Praze, dne 30. dubna 2024

…… ……

Manažer ISMS ***Ředitel Společnosti***