

Politika informační bezpečnosti – OpenOne a.s.

1 Úvod

Společnost **OpenOne a.s.** poskytuje moderní IT řešení a služby pro kontaktní centra a zákaznickou péči.

Bezpečnost informací našich zákazníků, partnerů i zaměstnanců je pro nás strategickou prioritou.

Naší strategií je provozovat systém řízení bezpečnosti informací (**ISMS**) v souladu s mezinárodní normou **ISO/IEC 27001:2022**, který nám pomáhá chránit cenná data, zajišťovat kontinuitu služeb a budovat dlouhodobou důvěru.

2 Závazek vedení

Vrcholové vedení společnosti OpenOne a.s. se zavazuje:

- zajišťovat **důvěrnost, integritu a dostupnost** všech informací,
 - uplatňovat požadavky platné legislativy a smluvních závazků (včetně principů vyplývajících z NIS2 / českého zákona o kybernetické bezpečnosti – ZoKB – v rozsahu relevantním pro naši společnost a naše zákazníky).
 - vytvářet podmínky pro efektivní fungování a rozvoj ISMS a **pravidelně školit vedení i** zaměstnance v oblasti kybernetické bezpečnosti,
 - podporovat **neustálé zlepšování** procesů informační bezpečnosti,
 - zajistit dostatečné zdroje pro řízení bezpečnosti a povědomí zaměstnanců.
-

3 Naše zásady

- **Ochrana informací** – informace chráníme před neoprávněným přístupem, ztrátou nebo poškozením.
- **Odpovědnost zaměstnanců** – každý zaměstnanec je seznámen se zásadami ISMS a odpovídá za jejich dodržování.
- **Řízení rizik** – pravidelně vyhodnocujeme rizika a přijímáme opatření ke snížení jejich dopadu.
- **Spolupráce s partnery** – od našich dodavatelů a partnerů vyžadujeme dodržování bezpečnostních principů a požadavků vycházejících z NIS2.
- **Incident management** – máme nastavené procesy pro rychlé odhalení, hlášení a řešení bezpečnostních incidentů, přičemž události s dopadem na zákazníky oznamujeme bez zbytečného odkladu dle dohodnutých SLA.
- **Business Continuity** – zajišťujeme provozní kontinuitu a připravenost na mimořádné situace (BCM/DR testy, definované RTO/RPO).
- **Ochrana osobních údajů** – nakládáme s osobními údaji v souladu s legislativou a zásadami GDPR.
- **Transparentnost a odpovědnost vedení** – představenstvo dozoruje řízení kybernetických rizik a schvaluje klíčová bezpečnostní opatření.

4 Naše cíle

- **Důvěra zákazníků** – budovat a udržovat důvěru klientů tím, že jejich data chráníme před ztrátou, únikem nebo zneužitím.
 - **Soulad s právními předpisy** – dodržovat legislativní a smluvní požadavky, zejména v oblasti ochrany osobních údajů (GDPR a podle potřeby také očekávání vyplývající z NIS2/ZoKB u našich zákazníků).
 - **Prevence a odolnost** – předcházet hrozbám a minimalizovat dopady bezpečnostních incidentů; pravidelně se zlepšovat na základě „lessons learned“.
 - **Dostupnost služeb** – zajišťovat kontinuitu poskytovaných služeb i v případě mimořádných událostí.
 - **Povědomí zaměstnanců** – školit a motivovat zaměstnance k odpovědnému chování v oblasti informační bezpečnosti.
 - **Neustálé zlepšování** – pravidelně vyhodnocovat účinnost bezpečnostních opatření a rozvíjet ISMS podle měnících se hrozeb a potřeb.
-

5 NIS2/ZoKB – veřejné prohlášení

- OpenOne a.s. provozuje **ISMS dle ISO/IEC 27001:2022** a **aktivně přizpůsobuje své procesy** očekáváním na kybernetickou odolnost, která vyplývají z rámce **NIS2/ZoKB** pro naše zákazníky v regulovaných sektorech.
- Jsme připraveni **včas informovat** zákazníky o významných incidentech, **koordinovat nápravné kroky** a vyžadovat přiměřené bezpečnostní požadavky i v dodavatelském řetězci.
- **Sledujeme vývoj legislativy** a veřejných metodik a potřebné změny promítáme do našich interních směrnic a školení vedení i zaměstnanců.

6 Závěr

Naším cílem je poskytovat **bezpečné a spolehlivé služby**, které chrání informace všech zainteresovaných stran a podporují naši pozici **důvěryhodného partnera** na trhu. Věříme, že kombinace certifikovaného ISMS a postupného přizpůsobování procesů očekáváním vyplývajícím z NIS2/ZoKB přináší našim zákazníkům i partnerům jasnou a srozumitelnou garanci odpovědného přístupu k bezpečnosti.