D10 – Politika bezpečnosti informací

Firma Aktivit spol. s r.o., při vědomí zásadního významu informací v dnešním světě, deklaruje svůj závazek pečlivě se věnovat oblasti bezpečnosti informací, poskytnout adekvátní zdroje a personální kapacity pro naplňování závazků v oblasti bezpečnosti informací a odhodlání systematicky řídit a zajišťovat bezpečnost informací v souladu s požadavky právních předpisů, dobré praxe v oboru a moderními trendy v oblasti zajišťování informační bezpečnosti a souvisejících činností a posilování schopnosti reagovat na aktuální bezpečnostní hrozby.

Aktivit spol. s r.o. proto buduje a neustále zlepšuje systém řízení bezpečnosti informací, aby chránila vlastní informační aktiva a aby všem zainteresovaným stranám, se kterými vstupuje do interakce, byla schopná garantovat nezbytnou míru bezpečí v této oblasti. Systém řízení bezpečnosti informací společnosti Aktivit je v souladu se zákonem č. 181/2014 Sb., o kybernetické bezpečnosti, a vyhláškou č. 82/2018 Sb., o kybernetické bezpečnosti, přičemž je současně připravován s ohledem na požadavky směrnice Evropského parlamentu a Rady (EU) 2022/2555 (NIS2).

Hlavním cílem politiky bezpečnosti informací firmy Aktivit je zajistit ochranu informačních aktiv firmy Aktivit tak, aby byla zachována důvěrnost, integrita a dostupnost informací a řízení informačních toků v souladu s platnou legislativou.

Závazek vedení firmy Aktivit:

Firma Aktivit se zavazuje, že bude prosazovat a uskutečňovat tuto politiku zejména:

- pravidelným monitorováním a vyhodnocováním bezpečnostních rizik a přijímáním odpovídajících bezpečnostních opatření,
- přijímáním opatření vedoucích k neustálému zlepšování bezpečnosti informací (tj. zabezpečení včasné dostupnosti), integrity (tj. zamezení nežádoucí modifikace informací) a důvěrnosti (tj. zamezení zneužití nebo ztráty informací),
- zajištěním pravidelného vzdělávání zaměstnanců firmy Aktivit a ostatních uživatelů informačních aktiv v oblasti bezpečnosti informací,
- stanovením a prosazováním způsobu zpracování informací, který definuje souborem vnitřních předpisů,
- dbá na to, aby náklady na bezpečnost byly vynakládány efektivně, tj. odpovídaly významu a ceně informací.

Odpovědnost zaměstnanců firmy Aktivit:

- zaměstnanec firmy Aktivit, kterému byl umožněn přístup k informačním aktivům, přebírá odpovědnost za bezpečné nakládání s těmito aktivy a za jejich ochranu,
- řídící dokumentace systému řízení bezpečnosti informací firmy Aktivit je závazná pro všechny uživatele informačních aktiv, a to bez ohledu na zastávanou funkci, pozici či roli ve firmě Aktivit,

- všichni uživatelé informačních aktiv nesou v souladu s platnou legislativou a interními předpisy zodpovědnost za dodržení, resp. porušení pravidel, s nimiž byli seznámeni,
- všichni uživatelé informačních aktiv jsou povinni předepsaným způsobem reagovat na bezpečnostní události a incidenty, které zjistí, a upozornit na ně v souladu s příslušnými vnitřními předpisy.

Hlavní zásady práce s informacemi ve firmě Aktivit a způsob jejich zabezpečení:

- zajistit ochranu osobních údajů v souladu s platnou legislativou,
- vytvářet a prosazovat systém řízeného přístupu k informacím,
- začleňovat zabezpečení informací do odpovědnosti za práci,
- zajišťovat zvyšování bezpečnostního povědomí a zvyšování kvalifikace zaměstnanců a ostatních uživatelů informačních aktiv v oblasti bezpečnosti informací,
- provádět neustálé monitorování a identifikaci bezpečnostních událostí a incidentů a přijímat účinná bezpečnostní opatření pro jejich eliminaci, a neustále zlepšovat bezpečnost informací.

Zaznamenané přestupky a neshody s výše uvedenými cíli hlásit na kompetentní osoby (Jednatel, manažer bezpečnosti informací, vedoucí IT oddělení, vedoucí oddělení)

Související podněty a informace můžete směřovat na adresu: info@aktivit.cz, případně ondrej.havrda@aktivit.cz

Datum poslední aktualizace: 26.11.2025

Provedl: Ing. Oskar Strnad

Schválil: Ing. Ondřej Válek