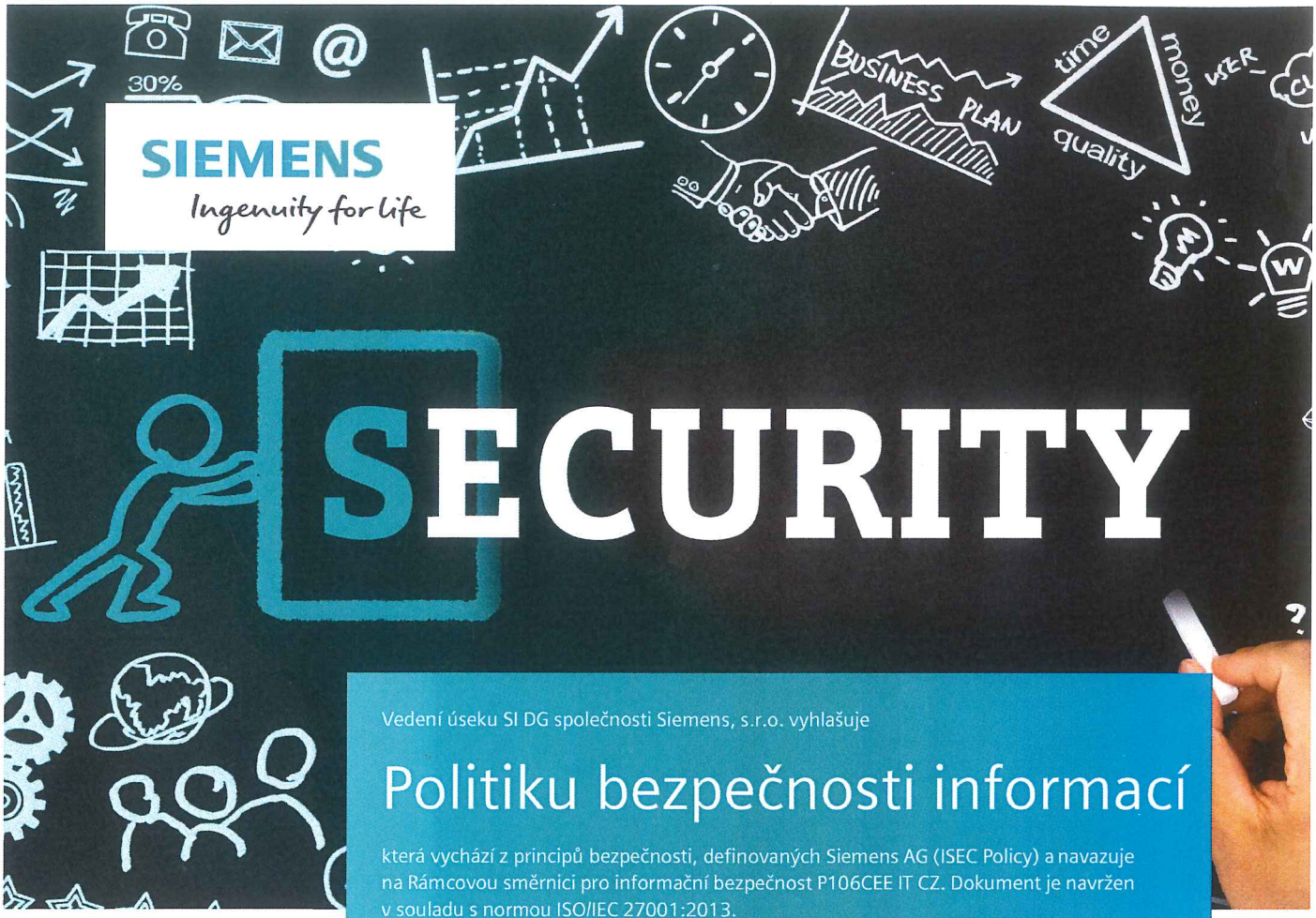


Vedení úseku SI DG společnosti Siemens, s.r.o. vyhlašuje

Politiku bezpečnosti informací

která vychází z principů bezpečnosti, definovaných Siemens AG (ISEC Policy) a navazuje na Rámcovou směrnici pro informační bezpečnost P106CEE IT CZ. Dokument je navržen v souladu s normou ISO/IEC 27001:2013.

Společnost Siemens, s.r.o. Smart Infrastructure, úsek Digital Grid (SI DG) si je vědom, jak důležitou roli hraje bezpečnost informací při podnikání. Zavedl proto Systém řízení bezpečnosti informací (Information Security Management System, ISMS), aby chránil svá informační aktiva a aby svým zákazníkům i partnerům poskytoval bezpečné služby. ISMS (stejně tak i tato politika) pokrývá všechny činnosti, vztahuje se na celou organizační strukturu úseku SI DG společnosti Siemens, s.r.o. a je platná pro všechny uživatele (zaměstnance a třetí strany).

Základní principy politiky bezpečnosti informací

- zajišťování bezpečnosti při spolupráci se zákazníky a obchodními partnery
- zajišťování bezpečnosti v oblasti elektronických bezpečnostních technologií a elektronických obchodních procesech
- zajišťování bezpečného přístupu a manipulace s informacemi

Základní a dlouhodobé cíle politiky bezpečnosti informací

Úsek SI DG důsledně zajišťuje ochranu informačních aktiv na potřebné úrovni tak, aby k nim měly přístup pouze oprávněné osoby (princip důvěrnosti), zajišťuje správnost a úplnost informací, jasně stanovil pravomoci a práva k jejich pozměňování (princip integrity) a zajišťuje, aby informace byly uživatelům přístupné v okamžiku jejich potřeby (princip dostupnosti). Efektivně řídí bezpečnostní incidenty a stanovuje opatření k jejich prevenci.

Plnění těchto cílů realizujeme definováním bezpečnostních standardů, jejich implementací a nastavením procesu kontroly a kontinuálního zlepšování.

Zásady bezpečnosti informací

Zaváděné bezpečnostní zásady a požadavky pro úsek SI DG a jeho zaměstnance jsou definovány v interních nařízeních a bezpečnostních směrnicích.

Zavazujeme se:

- dodržovat legislativní a smluvní požadavky
- řídit procesy a činnosti tak, aby byla zajištěna kontinuita a soulad s platnou legislativou České republiky i Evropské unie, mezinárodními smlouvami a jinými požadavky na ochranu bezpečnosti informací
- zajišťovat dostupnost informací v čase a místě dle potřeb úseku, ale pouze těm, kteří ji potřebují pro svoji pracovní činnost
- řídit integritu a životní cyklus informací od okamžiku jejich vzniku, předávání, užívání až po jejich likvidaci
- vzdělávat a rozvíjet naše zaměstnance, dodavatele a partnery v oblasti bezpečnosti informací
- považovat porušení pravidel informační bezpečnosti za hrubé porušení interních předpisů a smluvních vztahů
- zvyšovat účinnost našeho systému řízení bezpečnosti informací pravidelným monitorováním, přehodnocováním rizik, řízením bezpečnostních událostí a incidentů
- stanovovat nápravná a preventivní opatření a systém neustále zlepšovat

Zásady bezpečnosti informací dále zahrnují:

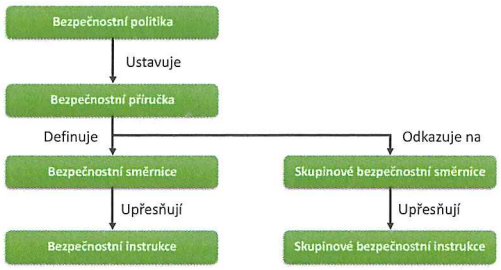
Hodnocení rizik a přijímání opatření k jejich pokrytí
Bezpečnostní opatření jsou přijímána na základě vyhodnocování hrozeb bezpečnosti informací prostřednictvím pravidelného hodnocení rizik.

Odpovědnosti
Opatření k zajištění bezpečnosti informací jsou prosazována s využitím bezpečnostních rolí:

- bezpečnostního manažera
- bezpečnostních správců
- vlastníků aktiv

Tyto role a uživatelé jsou odpovědni představiteli vedení pro ISMS – vedoucímu úseku. Problematika ISMS je pravidelně projednávána na poradách Security Committee. Vedení úseku zajišťuje dostupnost zdrojů (materiálních i lidských) potřebných pro provoz ISMS. Ostatní relevantní řídící role mohou být ustavovány dle potřeby v bezpečnostní dokumentaci.

Dokumentace
Dokumentace podporující a doplňující oblast politiky bezpečnosti informací je umístěna na lokálním intranetu Siemens, s.r.o. Obsahuje pravidla a procesy, které musí každý zaměstnanec dodržovat.
Dokumentace je vytvářena v českém jazyce, existující skupinové dokumenty jsou ponechány v jazyce anglickém, a je dostupná v následující struktuře:



Dokumenty jsou platné a účinné okamžikem publikování.

Pravidelné přezkoumávání ISMS
Zavedený ISMS je pravidelně 1x ročně přezkoumáván Security Committee k zajištění jeho efektivního fungování a stálého zlepšování.

Řešení neshod
Veškeré neshody ze zavedeného ISMS jsou identifikovány bezpečnostním manažerem, projednány na Security Committee a je zpracován návrh k jejich řešení.

Úsek SI DG a jeho vedení se touto politikou zavazují k zavedení všech bezpečnostních opatření směřujících ke splnění cílů a principů v oblasti bezpečnosti informací, dosahování zamýšleného výstupu ISMS a k neustálému zlepšování systému řízení bezpečnosti informací.

V Praze dne 01. 11. 2019

Ing. Zbyněk Bělina, Head of SI DG

Ing. Jiří Krátký, Head of finance SI DG