Příloha č. 1 – POLITIKA INFORMAČNÍ A KYBERNETICKÉ BEZPEČNOSTI

1. Závazek statutárních orgánů společností Skupiny ČEZ v oblasti informační a kybernetické bezpečnosti Skupiny ČEZ

Statutární orgány společností Skupiny ČEZ si uvědomují existenci reálných hrozeb v oblasti informační a kybernetické bezpečnosti a důležitost zajištění informační a kybernetické bezpečnosti ve Skupině ČEZ (dále jen IKB SKČ).

Statutární orgány společností Skupiny ČEZ si uvědomují svoji odpovědnost za IKB SKČ a proto se zavazují, že budou v souladu se strategií SKČ aktivně podporovat zajištění IKB SKČ.

Statutární orgány společností Skupiny ČEZ se zároveň budou aktivně podílet na hodnocení efektivnosti systému řízení a zajištění IKB SKČ a budou poskytovat odpovídající zdroje nutné k dosažení cílů IKB SKČ.

Pro adekvátní podporu zajištění IKB SKČ stanoví Představenstvo ČEZ, a. s., osobou odpovědnou za nastavení efektivního systému řízení IKB SKČ a zajištění adekvátních zdrojů k dosažení cílů IKB SKČ generálního ředitele ČEZ, a. s.

2. Odpovědnost za informační a kybernetickou bezpečnost Skupiny ČEZ

Generální ředitel ČEZ, a. s., deleguje dílčí odpovědnosti a s tím spojené pravomoci za nastavení efektivního systému řízení IKB SKČ a zajištění adekvátních zdrojů k dosažení cílů IKB SKČ v souladu se systémem řízení SKČ.

Za IKB SKČ odpovídají členové statutárních orgánů a zaměstnanci společností Skupiny ČEZ v rozsahu své pracovní náplně, svých odpovědností a kompetencí.

Vedoucí na všech úrovních řízení odpovídají za výkon kontrolních funkcí v oblasti IKB v rozsahu své působnosti.

3. Vize Skupiny ČEZ v oblasti informační a kybernetické bezpečnosti

Zajistit odpovídající úroveň IKB SKČ v souladu s platnou legislativou, mezinárodními standardy a doporučeními.

Zajistit spolehlivé poskytování produktů a služeb všem zákazníkům a partnerům SKČ a to pomocí kontinuálního vzdělávání a přípravy odborného personálu a všech uživatelů informací a informačních a technologických systémů, správy a rozvoje informačních a technologických systémů, efektivního řízení rizik a zavádění adekvátních bezpečnostních opatření.

4. Cíle v oblasti informační a kybernetické bezpečnosti Skupiny ČEZ

Hlavní cíle společností SKČ v oblasti IKB jsou zajistit, že:

- informační aktiva společností SKČ jsou odpovídajícím způsobem zabezpečena z hlediska jejich důvěrnosti, dostupnosti a integrity,
- bezpečnostní rizika informačních aktiv spojených s chodem společností SKČ jsou efektivně řízena,
- jsou nastaveny a kontrolovány efektivní procesy k zajištění IKB,
- bezpečnostní opatření jsou v souladu s platnou legislativou a mezinárodními standardy a doporučeními.

Hlavní cíle jsou podporovány následujícími dílčími cíli:

- Implementovat Politiku IKB SKČ, jako předpoklad pro zajištění přiměřené úrovně IKB SKČ.

- Vybudovat a neustále zlepšovat systém řízení IKB dle nejlepší profesní praxe a platné legislativy.
- Zajistit odpovědnost všech zaměstnanců za IKB v rozsahu jejich pracovní náplně a jejich odpovědností a kompetencí.
- Efektivně řídit rizika IKB v kontextu podnikatelských aktivit společností SKČ a implementovat opatření pro snižování rizik IKB na akceptovatelnou úroveň.
- Zajišťovat bezpečnost a spolehlivost provozovaných informačních a technologických systémů a aplikací.
- Průběžně zajišťovat konsolidaci bezpečnostních funkcí a bezpečnostních aplikací a jejich postupné zlepšování a zefektivňování.
- Průběžně zapracovávat požadavky IKB do všech procesů, projektů a změn.
- Zvyšovat bezpečnostní povědomí zaměstnanců, uživatelů systémů, odběratelů služeb a prostřednictvím systému vzdělávání je vést k dodržování zásad IKB.
- Efektivně řídit přístup k informacím, informačním a technologickým systémům tak, aby byla zajištěna přiměřená úroveň jejich ochrany.
- Bezpečně umísťovat důležitá informační aktiva a zajistit jejich fyzickou ochranu.
- Zajistit detekci, eskalaci a zvládnutí bezpečnostních incidentů v oblasti IKB s důrazem na prevenci.
- Monitorovat interní a externí perimetry IKB SKČ s cílem identifikovat možný útok dřív, než nastane.
- Zajistit kontinuální dostupnost informačních a technologických systémů i v případě náhlého výpadku a to implementací procesu řízení kontinuity činností.

Jednotlivé bezpečnostní cíle se naplňují pomocí zavádění adekvátních personálních, organizačních, procesních či technických opatření, určených v rámci procesu řízení rizik a v souladu s legislativními požadavky a relevantními standardy či normami.

5. Rozsah a hranice systému řízení informační a kybernetické bezpečnosti Skupiny ČEZ

Systém řízení IKB SKČ se vztahuje na všechna pracoviště společností SKČ, členy statutárních orgánů a všechny zaměstnance společností SKČ, všechny podnikatelské aktivity a know-how SKČ, i na služby a výrobky poskytované externími dodavateli.

Systém řízení IKB SKČ zahrnuje tyto oblasti:

- Politiky bezpečnosti informací (Information security policies)
- Organizace bezpečnosti informací (Organization of information security)
- Bezpečnost lidských zdrojů (Human resource security)
- Řízení aktiv (Asset management)
- Řízení přístupu (Access control)
- Kryptografie (Cryptography)
- Fyzická ochrana a bezpečnost prostředí (Physical and environmental security)
- Bezpečnost provozu (Operations security)
- Bezpečnost komunikací (Communications security)
- Akvizice, vývoj a údržba systémů (System acquisition, development and maintenance)
- Vztahy s dodavateli (Supplier relationships)
- Zvládání incidentů bezpečnosti informací (Information security incident management)
- Aspekty informační bezpečnosti v oblasti řízení kontinuity činností (Information security aspects of business continuity management)
- Soulad s požadavky (Compliance)

Systém řízení IKB se přiměřeně uplatňuje i na informace a informační systémy, jejichž ochrana je upravena zvláštními zákony, přičemž požadavky zvláštních zákonů mají před obecnou úpravou IKB SKČ přednost.