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.

2 – POLITIKA OCHRANY INFORMACÍ, PROJEKTŮ A ZÁJMŮ

1. Závazek statutárních orgánů společností Skupiny ČEZ v oblasti ochrany informací projektů a zájmů Skupiny ČEZ

Statutární orgány společností Skupiny ČEZ si uvědomují existenci reálných hrozeb v oblasti ochrany informací, projektů a zájmů a důležitost zajištění ochrany informací, projektů a zájmů ve Skupině ČEZ (dále jen SKČ).

Statutární orgány společností Skupiny ČEZ si dále uvědomují svoji odpovědnost za oblast ochrany informací projektů a zájmů v SKČ a proto se zavazují, že budou v souladu se strategií SKČ aktivně podporovat zajištění ochrany informací, projektů a zájmů SKČ.

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

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

2. Odpovědnost za ochranu informací, projektů a zájmů Skupiny ČEZ

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

Za ochranu informací, projektů a zájmů 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 ochrany informací, projektů a zájmů v rozsahu své působnosti.

3. Vize Skupiny ČEZ v oblasti ochrany informací, projektů a zájmů Skupiny ČEZ

Zajistit odpovídající úroveň ochrany informací, projektů a zájmů 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 ochrany informací, projektů a zájmů ve Skupině ČEZ

Hlavní cíle společností SKČ v oblasti ochrany informací, projektů a zájmů jsou:

- dodržení a naplnění legislativy v oblasti ochrany informací, zejména ochrany osobních údajů, obchodního tajemství a utajovaných informací,
- 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,
- přijímat bezpečnostní opatření na principu posouzení závažnosti vyhodnocených rizik, jejich dopadů a ekonomické náročnosti opatření.

Hlavní cíle jsou podporovány následujícími dílčími cíli:

- zajištění realizace Politiky ochrany informací, projektů a zájmů ve všech společnostech Skupiny ČEZ za účelem zajištění jednotného standardu ochrany informací,
- implementace a realizace legislativních požadavků na ochranu osobních údajů plynoucích zejména z nařízení EU 2016/679 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES,
- naplnění požadavků zákona č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti ve znění pozdějších předpisů,
- vysoké povědomí zaměstnanců společnosti o významu ochrany informací, zejména pak obchodního tajemství a ochrany osobních údajů,
- zvyšování účinnost systému ochrany informací, projektů a zájmů pravidelným monitorováním, hodnocením rizik, řízením bezpečnostních událostí a incidentů prostřednictvím nápravných a preventivních opatření,
- prosazování politiky bezpečného pracoviště, tj. politiky čistého stolu a prázdné obrazovky,
- zajištění ochrany klíčových osob a nositelů chráněných informací, know-how a rozhodovacích pravomocí.,
- detekce bezpečnostních incidentů v oblasti ochrany informací, projektů a zájmů a jejich řešení s následným přijetím opatření zejména systémové povahy.

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 ochrany informací, projektů a zájmů Skupiny ČEZ

Systém řízení ochrany informací, projektů a zájmů 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 ochrany informací, projektů a zájmů 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 (např. problematika utajovaných informací dle zákona č. 412/2005 Sb., o ochraně utajovaných informací a bezpečnostní způsobilosti, ve znění pozdějších předpisů je řešena samostatnou řídicí dokumentací).

3 – POLITIKA ZABEZPEČENÍ JZ A JM A OCHRANY KRITICKÉ INFRASTRUKTURY

1. Závazek statutárních orgánů společností Skupiny ČEZ v oblasti zabezpečení JZ a JM a ochrany kritické infrastruktury

Statutární orgány společností Skupiny ČEZ si uvědomují existenci reálných hrozeb v oblasti zabezpečení JZ a JM a ochrany kritické infrastruktury a důležitost zajištění zabezpečení JZ a JM a ochrany kritické infrastruktury.

Statutární orgány společností Skupiny ČEZ si současně uvědomují svoji odpovědnost za zajištění zabezpečení JZ a JM a ochrany kritické infrastruktury, a proto se zavazují, že budou v souladu se strategií SKČ aktivně podporovat zajištění zabezpečení JZ a JM a ochranu kritické infrastruktury.

Statutární orgány společností Skupiny ČEZ se zároveň budou aktivně podílet na hodnocení efektivnosti systému řízení a zajištění zabezpečení JZ a JM a ochrany kritické infrastruktury a budou poskytovat odpovídající zdroje nutné k dosažení cílů zabezpečení JZ a JM a ochrany kritické infrastruktury.

Pro adekvátní podporu zajištění zabezpečení JZ a JM a ochrany kritické infrastruktury stanoví Představenstvo ČEZ, a. s., osobou odpovědnou za nastavení efektivního systému řízení zabezpečení JZ a JM a ochrany kritické infrastruktury a zajištění adekvátních zdrojů k dosažení cílů zabezpečení JZ a JM a ochrany kritické infrastruktury generálního ředitele ČEZ, a. s.

2. Odpovědnost za zajištění zabezpečení JZ a JM a ochrany kritické infrastruktury

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

Za zabezpečení JZ a JM a ochranu kritické infrastruktury 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 zabezpečení JZ a JM a ochrany kritické infrastruktury v rozsahu své působnosti.

3. Vize Skupiny ČEZ v oblasti zabezpečení JZ a JM a ochrany kritické infrastruktury

Zajistit taková organizační a technická opatření, která vyloučí, případně v maximální míře omezí rizika protiprávního jednání představujícího hrozbu pro výrobní zařízení a majetek společnosti. Opatření pro zabezpečení JZ a JM musí zabránit krádeži jaderných materiálů z JZ nebo provedení radiologické sabotáže na JZ a zmírňovat následky těchto skutečností. Rozsah a způsob zabezpečení JZ a JM musí být stanoven s ohledem na aktuální projektovou hrozbu, musí být realizován v souladu s platnou legislativou a maximálně reflektovat mezinárodní standardy a doporučení.

4. Cíle v oblasti zabezpečení JZ a JM a ochrany kritické infrastruktury

Hlavní cíle společností SKČ v oblasti zabezpečení JZ a JM a ochrany kritické infrastruktury jsou:

- musí být efektivně a účinně bráněno přístupu neoprávněných osob do střežených prostorů výrobních zařízení
- musí být zabráněno vzniku neoprávněných činností (krádež nebo sabotáž) s jadernými materiály, jaderným zařízením a vybranými položkami
- musí být zajištěna taková úroveň zabezpečení JZ a JM a ochrany kritické infrastruktury napříč souvisejícími procesy tak, aby rizika z činností společností SKČ byla na přijatelné úrovni, která umožní plnit poslání společností a realizovat přiměřený zisk
- musí být udržován takový stav zařízení a personálu zabezpečení JZ a JM a ochrany kritické infrastruktury, který je považován státními dozornými orgány a odbornou veřejností za akceptovatelný
- proces řízení a organizace zabezpečení JZ a JM a ochrany kritické infrastruktury musí být řízen efektivně a musí být nastaveny dostatečné nezávislé kontrolní mechanismy

Hlavní cíle jsou podporovány následujícími dílčími cíli:

- Implementovat Politiku zabezpečení JZ a JM a ochrany kritické infrastruktury, jako předpoklad pro zajištění akceptovatelné úrovně zabezpečení JZ a JM a ochrany kritické infrastruktury.
- Neustále zlepšovat systém řízení zabezpečení JZ a JM a ochrany kritické infrastruktury dle nejlepší profesní praxe a platné legislativy.
- Zajistit odpovědnost zaměstnanců za zajištění zabezpečení JZ a JM a ochrany kritické infrastruktury v rozsahu jejich pracovní náplně a jejich odpovědností a kompetencí.
- Efektivně řídit rizika zabezpečení JZ a JM a ochrany kritické infrastruktury v kontextu podnikatelských aktivit společností SKČ a implementovat opatření pro snižování rizik v oblasti zabezpečení JZ a JM a ochrany kritické infrastruktury na akceptovatelnou úroveň.
- Průběžně zapracovávat požadavky zabezpečení JZ a JM a ochrany kritické infrastruktury do relevantních procesů, projektů a změn.
- Zvyšovat bezpečnostní povědomí zaměstnanců a prostřednictvím systému vzdělávání je vést k dodržování zásad a pravidel zabezpečení JZ a JM a ochrany kritické infrastruktury.
- Zajistit detekci, eskalaci a zvládnutí bezpečnostních incidentů v oblasti zabezpečení JZ a JM a ochrany kritické infrastruktury s důrazem na prevenci.

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 zabezpečení JZ a JM a ochrany kritické infrastruktury

Systém řízení zabezpečení JZ a JM a ochrany kritické infrastruktury se vztahuje na členy statutárních orgánů, na garanty procesů a další vedoucí, kteří zajišťují činnosti související s oblastí řízení zabezpečení JZ a JM a ochrany kritické infrastruktury. Výstupy procesu – stanovené bezpečnostní požadavky pro oblast zabezpečení JZ a JM a ochrany kritické infrastruktury jsou závazné pro všechny zaměstnance SKČ a zaměstnance dodavatelů, kteří vykonávají činnosti v rámci SKČ.