Bezpečnostní politika skupiny Sev.en Energy (výtah)

Tento dokument definuje základní organizační, řídící a kontrolní opatření, směřujících k zajištění jednotného systému řízení bezpečnostních rizik (dále také „bezpečnost“) ve skupině Sev.en Energy (dále také „Skupina“) na všech úrovních řízení.

Základní principy řízení bezpečnostních rizik ve skupině Sev.en Energy

Účel a oblast úpravy

Bezpečnostní politika je chápána jako celek složený z jednotlivých opatření, zejména pak z organizace a řízení, řízení aktiv, administrativní, fyzické, personální, informační a kybernetické bezpečnosti s cílem zajistit dostupnost, integritu a důvěrnost aktiv Skupiny.

Bezpečnostní politika se dotýká zaměstnanců Skupiny, externích dodavatelů, odběratelů, všech informací, které Skupina zpracovává a uchovává v prostorách Skupiny nebo mimo ně, movitého i nemovitého majetku, jakož i ostatních aktiv, které mohou být ohroženy bezpečnostním rizikem.

Bezpečnostní politika je závazná pro všechny společnosti Skupiny, jednotlivé organizační útvary a zaměstnance. Tato politika se přiměřeně vztahuje i na externí subjekty, které jsou ve smluvním vztahu ke Skupině.

Řízení bezpečnostních rizik je nedílnou součástí systému řízení strategických, finančních, operačních a legislativních rizik.

Prohlášení

Skupina vyjadřuje touto bezpečnostní politikou svoji strategii trvalého zajišťování řízení bezpečnosti, která je součástí řídících procesů.

K prosazení zásad bezpečnosti do vědomí všech zaměstnanců musí být trvale realizován program budování bezpečnostního povědomí všech zaměstnanců Skupiny.

Základní cíle řízení bezpečnosti

Základními cíli v oblasti řízení bezpečnosti jsou ochrana života a zdraví zaměstnanců, případně dalších osob, naplňování požadavků relevantních zákonů a dalších předpisů, podpora plnění obchodních zájmů Skupiny,

naplňování požadavků vyplývajících ze smluvních vztahů, ochrana informací, ochrana majetku a ochrana dobrého jména Skupiny.

Základní principy řízení bezpečnosti

Všichni zaměstnanci jsou odpovědni za zajišťování bezpečnosti aktiv Skupiny.

Přijímaná bezpečnostní opatření musí být přiměřená riziku, tedy pravděpodobnosti vzniku škody, jejím dopadům a hodnotě aktiva.

Činnosti související s řízením bezpečnosti musí být centrálně řízeny a koordinovány.

Pro řízení bezpečnosti musí být vytvořen systém řízení bezpečnostní dokumentace a záznamů na podporu prováděných činností.

Pro provoz a zlepšování systému řízení bezpečnosti musí být zajištěny dostatečné finanční, materiálové a personální zdroje.

Výkon činností související se systémem řízení bezpečnosti musí být pravidelně kontrolován a vyhodnocován. Musí být přijímána opatření k jeho zlepšování s důrazem na reakci na nové hrozby, zranitelnosti a aktiva.

Zásady řízení bezpečnosti: organizace a řízení bezpečnosti

Přidělení kompetencí a odpovědností za řízení bezpečnosti.

Stanovení koordinačního rámce.

Definování schvalovacího procesu prostředků pro zpracování informací.

Zajištění ochrany informací ve smlouvách s externími subjekty a zajištění spolupráce s externími subjekty v oblasti ochrany aktiv Skupiny.

Řízení bezpečnostních rizik s externími subjekty včetně identifikace rizik spojených s jejich přístupem, zajištění bezpečného přístupu zaměstnanců externích subjektů k informacím a ostatním aktivům Skupiny a zavázání těchto stran k dodržování požadavků Skupiny na zabezpečení informací a ostatních aktiv Skupiny.

Bezpečnostní politika podléhá jak plánovanému přezkumu, tak neplánovanému dle potřeby Skupiny.

Zásady řízení bezpečnosti: řízení aktiv

Cílem řízení aktiv je nastavit a udržovat přiměřenou ochranu aktiv Skupiny s důrazem na jejich klasifikaci. Cílem klasifikace aktiv je zajištění přiměřenosti ochrany aktiv. Aktiva musí být klasifikována na základě jejich potřebnosti a důležitosti pro Skupinu.

Veškerá aktiva zařazená do systému řízení bezpečnosti musí být ohodnocena a musí být určen jejich garant. Za identifikaci a ohodnocení aktiv odpovídají garanti aktiv. S aktivy Skupiny musí být nakládáno způsobem zohledňujícím možná rizika, která s těmito aktivy souvisejí.

Pro účely klasifikace informačních aktiv je stanoveno třístupňové klasifikační schéma. Klasifikace technických aktiv upravuje zvláštní metodika.

Zásady řízení bezpečnosti: personální bezpečnost

Cílem personální bezpečnosti je snížit riziko lidské chyby, neetického nebo protiprávního jednání s dopadem na aktiva Skupiny.

Všechny pracovní pozice musí být zařazeny do rizikových stupňů dle vybraných rizikových kritérií.

U nově přijímaných zaměstnanců musí být minimalizována rizika, která jsou spojena se zkreslenými, zatajenými, nepravdivými nebo neúplnými údaji, které uchazeč o zaměstnání předložil.

Všichni nově přijímaní zaměstnanci musí absolvovat vstupní školení k problematice bezpečnosti a ochraně aktiv.

Všichni zaměstnanci musí absolvovat pravidelně školení k problematice bezpečnosti a ochraně aktiv.

U vybraných pracovních pozic (v závislosti na rizikovém stupni) musí být zajištěno doplňkové vzdělávání v oblasti bezpečnosti.

Všichni vedoucí zaměstnanci musí vyžadovat po svých podřízených a případně po externích smluvních subjektech, dodržování bezpečnostních zásad.

V případě porušení bezpečnostní politiky a související dokumentace bude vůči zaměstnancům vyvozována právní odpovědnost.

Při ukončení zaměstnaneckého poměru, případně smluvního vztahu musí být jasně stanoveny odpovědnosti za úpravu přístupových oprávnění resp. za bezpečné předání svěřených aktiv.

Zásady řízení bezpečnosti: fyzická bezpečnost

Cílem fyzické bezpečnosti je předcházet neautorizovanému přístupu, poškození a zásahům do aktiv Skupiny.

Veškerá pracoviště, v nichž jsou uchovávána aktiva Skupiny nebo v nichž se s nimi zachází, musí být zabezpečeny pomocí příslušných fyzických bezpečnostních opatření. Důraz je položen na definování a zajištění ochrany zabezpečených oblastí.

Zabezpečené oblasti jsou chráněny přiměřenými kontrolami vstupu tak, aby bylo zajištěno, že osoba, která vstupuje do zabezpečených oblastí, má ke vstupu oprávnění.

V případě změnových řízení, která se dotýkají pracovišť Skupiny, musí být zohledněna bezpečnostní rizika ohrožující aktiva v nich umístěná.

Zařízení zpracovávající informace musí být umísťována tak, aby se minimalizovalo riziko působení vnějších vlivů a neautorizovaného přístupu.

Zařízení zpracovávající informace musí být fyzicky chráněna v závislosti na klasifikačním stupni informací jimi zpracovávaných. Zařízení musí být též chráněna před výpadkem elektrického proudu nebo jinými anomáliemi napájení.

Oprava nebo likvidace zařízení, případně nosiče informací, na nichž byly zpracovávány klasifikované informace, musí být prováděna takovým způsobem, aby zaměstnancem Skupiny, nebo zaměstnancem externího subjektu nebylo možné získat z tohoto zařízení informace, které na něm byly zpracovávány, a s nimiž tito zaměstnanci nejsou oprávněni se seznamovat.

Zásady řízení bezpečnosti: řízení komunikací a řízení provozu

Cílem řízení komunikací a řízení provozu je zajistit správný a bezpečný provoz prostředků pro zpracování informací.

Řízení komunikací a provozu je realizováno prostřednictvím opatření v zejména v oblasti provozních postupů a odpovědností, řízení dodávek služeb externích subjektů, plánování a přejímání informačních systémů, ochrany proti škodlivým programům a mobilním kódům, zálohování, bezpečnosti při zacházení s médii, výměně informací a monitoringu.

Zásady řízení bezpečnosti: řízení přístupů

Cílem řízení přístupů je zejména zajistit oprávněný přístup uživatelů, předcházet neoprávněnému uživatelskému přístupu k síťovým službám, operačním systémům, řídicím systémům a k informacím uložených v informačním systému.

Řízení přístupu uživatelů k informacím a službám informačních systémů Skupiny musí být prováděno na základě přidělených rolí a přístupových práv do jednotlivých informačních systémů, v souladu s klasifikací a řízením aktiv, v souladu s formálními postupy registrace uživatelů a správy přístupu zaměřenými na přidělení, změnu a odebrání přístupu a v souladu s postupy správy systému přístupu jednotlivých informačních systémů.

Všichni uživatelé musí být seznámeni se svými povinnostmi, pravidly a postupy užívání přístupu k informačním systémům Skupiny s důrazem na

používání uživatelských hesel a jiných autentizačních prostředků a ochranu neobsluhovaných aplikací, služeb a zařízení při přerušení nebo ukončení práce.

V rámci informačních systémů musí být pro jednotlivé části stanoveny a prosazovány způsoby a postupy monitorování včetně stanovení rozsahu, ochrany a vyhodnocování auditních záznamů a časové synchronizace.

Použití mobilních zařízení pro práci s informačními systémy na dálku, vzdálený přístup k vnitřním informačním systémům a cloudovým službám musí být řízen.

Zásady řízení bezpečnosti: akvizice, vývoj a údržba informačních systémů

Akvizice, vývoj a údržba informačních systémů jsou realizovány zejména prostřednictvím bezpečnostních požadavků na informační systémy, správného zpracování v aplikacích, kryptografických opatření, bezpečnosti systémových souborů, bezpečnosti procesů vývoje a údržby a řízení technických zranitelností

Zásady řízení bezpečnosti: řízení bezpečnostních incidentů

Řízení bezpečnostních incidentů zahrnuje zejména hlášení bezpečnostních incidentů, stanovení odpovědností a postupů pro zvládání bezpečnostních incidentů, informování odpovědných osob o vzniku a řešení bezpečnostních incidentů, provádění ponaučení z bezpečnostních incidentů a shromažďování důkazů.

Veškeré bezpečnostní incidenty ve Skupině musí být centrálně řízeny a spravovány.

Zásady řízení bezpečnosti: řízení kontinuity činností

Cílem řízení kontinuity činností Skupiny je zabránit přerušení činností a chránit Skupinu před následky závažných chyb, katastrof a nepředvídatelných událostí nebo tyto následky minimalizovat. Důraz je položen na ochranu kritických procesů.

Systém zajištění kontinuity činností zahrnuje zejména provedení analýzy dopadů k určení rizik pro strategické cíle, včetně identifikace a určení priorit kritických procesů, identifikaci aktiv, která se účastní kritických procesů, vytvoření systému řízení kontinuity činností s důrazem na stanovení strategie, určení a obsazení rolí zajišťující chod systémů, návrhy postupů pro zachování kontinuity činností a jejich zdokumentování v plánech kontinuity činností a provádění testování a aktualizace plánů kontinuity činností.

Zásady řízení bezpečnosti: soulad s požadavky

Cílem souladu s požadavky je zejména vyvarovat se porušení norem trestního nebo občanského práva, zákonných nebo smluvních povinností.

Zajištění souladu s požadavky zahrnuje definování a zdokumentování všech relevantních právních a smluvních požadavků.

Je nutné zajistit monitoring připravované relevantní legislativy.

Zásady řízení bezpečnosti: kritéria hodnocení bezpečnostních rizik

Hodnocení úrovně bezpečnostního rizika je určováno na základě hodnoty aktiva a stanovení úrovně četnosti hrozby a dopadu hrozby. Hodnocení rizik se provádí s využitím analýzy rizik.

Hodnocení úrovně bezpečnostního rizika je prováděno na základě stanovení hodnoty jednotlivých aktiv Skupiny, na základě požadavků relevantní legislativy a požadavků vyplývajících z uzavřených smluvních vztahů, na základě možných dopadů identifikovaných hrozeb a četnosti identifikovaných hrozeb.

Kompetenční a odpovědnostní rámec

Kompetence a odpovědnosti jsou v systému řízení bezpečnostních rizik přiřazeny jednak funkcím v organizační struktuře Skupiny a dále bezpečnostním rolím.

Nejvyšším orgánem řízení bezpečnosti je CEO Skupiny.

Rozsah a obsah předpisů navazujících na bezpečnostní politiku určuje bezpečnostní ředitel Skupiny.