Elektrárny Opatovice, a.s. EOP Distribuce, a.s.	Politika č. 1/2021 – 1 **VEŘEJNÉ**	Datum účinnosti revize: 20. 1. 2023
Účinnost: 1. 6. 2021	Věc:	Spis. zn.: 2.92
Přílohy: 0	Politika kybernetické bezpečnosti skupiny EPIF	Zpracoval: Ing. V. Vítek
Za revize odpovídá: Tajemník společnosti		Počet stran: 6 vč. příloh: 6

POLITIKA KYBERNETICKÉ BEZPEČNOSTI SKUPINY EPIF

Schválil:

…… ……

výkonná ředitelka za Elektrárny Opatovice, a.s.

ředitel společnosti za EOP Distribuce, a.s.

Přezkoumal formálně: Přezkoumal věcně:

....

správce OŘN finanční ředitel

- Výtisky nejsou součástí řízené dokumentace.
- Pravidla klasifikace, označování a ochrany informací/dokumentů v EOP/DTO jsou upravena ve Spisovém řádu.

PŘEHLED REVIZÍ

- Číslem v postupné řadě ve sloupci "revize č." jsou označovány pouze revize spojené se změnou dokumentu.
- Periodické revize aktuálnosti (beze změny dokumentu) jsou označovány ve sloupci "revize č." zkratkou PR (bez postupného čísla). Datum periodické revize, jméno a podpis zástupce útvaru odpovědného za revizi uveďte ve sloupci "předmět změny".

Revize č.	Předmět změny (kapitola, článek)	Strany	Datum účinnosti	Podpis správce dokumentu:
1	Formální úprava pro EOP i DTO (po odštěpení) + 5.1 Související int. normy	celý dokument	20. 1. 2023	

Revize č.	Vypracoval jméno	podpis	Přezkoumal jméno	podpis	Schválil jméno	podpis
1	V. Vítek				R. Zadrobílková K. Čipera	

Obsah:

1 ÚČEL

Tato politika implementuje „Zásady kybernetické bezpečnosti“ skupiny EP INFRASTRUCTURE (dále jen „EPIF“) do interních předpisů společnosti Elektrárny Opatovice, a.s. a EOP Distribuce, a.s..

Tato Politika stanoví hlavní bezpečnostní zásady skupiny EPIF a zavazuje všechny zaměstnance k provádění veškerých činností při nakládání s informacemi a při využívání technologií a digitálních služeb se zvláštním důrazem na ochranu informací a k reagování na nové bezpečnostní hrozby, regulatorní požadavky a neustále se rozvíjející prostředí informačních technologií.

2 PŮSOBNOST

Pravidla a postupy stanovené touto politikou jsou platné ve společnosti Elektrárny Opatovice, a.s. (dále jen EOP) a EOP Distribuce, a.s. (dále jen DTO).

3 PROHLÁŠENÍ

Společnosti ve skupině EPIF musí dodržovat přinejmenším níže uvedené klíčové zásady kybernetické bezpečnosti a odpovídají za výběr a implementaci konkrétních bezpečnostních opatření tak, aby tyto zásady dodržely.

Tam, kde je to možné, je třeba využívat znalostí a zkušeností ostatních společností ve skupině EPIF.

Problematiku kybernetické bezpečnosti společnost detailněji upraví v dalších interních normách, které v rámci revizí tohoto dokumentu konkretizuje v bodě 5.1 tak, jak budou postupně implementovány v rámci zavádění systému řízení informační bezpečnosti (ISMS).

Pokud některé z níže uvedených zásad není možné v době implementace této politiky dodržet s ohledem na nutnost zajištění určitých technických či organizačních opatření, budou tato opatření zahrnuta do plánu opatření k zajištění kybernetické bezpečnosti.

4 KLÍČOVÉ ZÁSADY KYBERNETICKÉ BEZPEČNOSTI

A. **Organizace a řízení bezpečnosti.** Vytvořen by měl být efektivní systém řízení bezpečnosti pro všechny bezpečnostní oblasti ve společnosti. Do systému musí být zapojeno i nejvyšší vedení organizace a musí poskytovat nezbytnou součinnost.

B. **Hodnocení rizik.** Na základě pravidelného posuzování rizik se stanoví úroveň přijatelného rizika v organizaci.

C. **Bezpečnostní politiky.** Společnost implementuje a schvaluje politiky v oblasti informační bezpečnosti a řádně s nimi seznámí všechny zaměstnance a příslušné externí subjekty. V návaznosti na organizační změny a výsledky hodnocení rizik aktualizuje politiku bezpečnosti informací a konkrétně zaměřené bezpečnostní politiky.

D. **Informovanost v oblasti bezpečnosti.** Společnost zvyšuje povědomí svých zaměstnanců o bezpečnosti prostřednictvím pravidelných povinných školení. Tuto povinnost uplatňuje i ve vztahu k příslušným externím subjektům, které mají přístup do vnitřních informačních systémů organizace, případně ji s nimi upravuje smluvně.

E. **Správa aktiv.** Společnost identifikuje důležitá aktiva, spravuje vlastnická práva k nim, stanoví vhodnou úroveň jejich ochrany a odpovídajícím způsobem s nimi nakládá.

F. **Správa identit a řízení přístupů.** V rámci řízení přístupů společnost implementuje správu identit pro účely automatického poskytování a rušení uživatelských účtů, správy hesel, jednotného přihlašování (Single Sign-On nebo SSO) a řízení přístupu na základě role (Role-Based Access Control nebo RBAC). Společnost zavádí postupy a opatření pro omezení přístupu uživatelů k informačním systémům a snižuje rozsah jejich povolených činností na nezbytné minimum, které vyžadují dané uživatelské role. Zvláštní pozornost je věnována privilegovaným uživatelům a sdíleným účtům, není-li možné je eliminovat.

G. **Bezpečné propojení a vzdálená pracoviště.** Aby bylo zajištěno bezpečné připojení z vnitřní sítě nebo prostřednictvím vzdáleného přístupu z vnějších či veřejných sítí k IT prostředí organizace, je zavedena ochrana zařízení koncových uživatelů, mobilních zařízení, serverů a řídicích systémů. Pro přístup do vnitřní sítě zvenčí je přednostně využíván dvouúrovňový ověřovací mechanismus.

H. **Ochrana před škodlivým softwarem**. Společnost řeší kontrolu škodlivého softwaru, zavádí analytické nástroje, případně metody filtrování (e-mail, internet, síť). Společnost definuje příslušné postupy a zaměřuje se na zvyšování pozornosti uživatelů vůči phishingovým a podobným útokům a její testování.

I. **Správa hrozeb a zranitelných míst.** Společnost využívá postupy a podle dané situace i technické prostředky pro detekci incidentů a preventivní zmírňování skutečných hrozeb a zranitelností.

J. **Sledování a průběžné vyhodnocování rizik.** Společnost má zavedeny postupy a technické prostředky pro monitoring informačních systémů, řídicích systémů, podezřelých aktivit v síti a neobvyklého chování uživatelů. Zásadní význam má účinná průběžná, respektive pravidelná, analýza výsledků sledování.

K. **Patch management a bezpečná konfigurace.** Společnost vytváří postupy a evidence, které zajišťují aktualizace a opravy na zařízeních a tím dodržování zavedených standardů pro bezpečné nastavení.

L. **Bezpečnost sítě.** V zájmu ochrany své sítě se společnost zaměřuje na bezpečnost v síťové architektuře a rozděluje síť na technickou, provozní oblast a oblast rizik, jednoznačně definuje charakteristiky perimetru sítě a přístupová pravidla. Síťový provoz mezí sítí a vnějšími sítěmi, externími partnery a u vzdálených připojení je řízen prostřednictvím autorizací, případně zabezpečení DMZ a filtrování síťového provozu.

M. **Kybernetická odolnost.** Společnost uplatní postupy pro efektivní odezvu na incidenty v souladu s plány řízení incidentů a postupy pro obnovu provozu po haváriích. Určí zaměstnance pověřené řešením incidentů. Společnost pravidelně testuje svou odolnost prostřednictvím nezávislých hodnocení zabezpečení a penetračního testování. Za účelem zmírnění útoků vyděračských softwarů jsou implementovány silné mechanismy na ochranu a ukládání dat.

N. **Kontinuita provozu.** Společnost vytváří a ověřuje plán zajištění kontinuity provozu, aby byla schopna zachovat obchodní funkce a základní služby IT v nepříznivých situacích, např. v případě krizí, katastrof, závažných útoků na informační technologie či incidentů.

O. **Spolehlivý dodavatelský řetězec.** Před poskytnutím přístupu ke svým citlivým informačním aktivům společnost zakotví bezpečnostní požadavky ve všech smlouvách s externími subjekty a pravidelně tyto smluvní požadavky a jejich plnění vyhodnocuje.

P. **Fyzická ochrana.** Společnost využívá k ochraně veškerých kritických zabezpečených či provozních oblastí fyzické překážky, jako jsou zdi, vstupní kontroly, např. prostřednictvím elektronicky řízených vstupních bran, bezpečnostních rentgenů, pracovníků recepce,

speciálních zámků, případně obrazovek. Vstup do vnitřních kanceláří je povolen pouze oprávněným osobám, a to za podmínek a s využitím opatření, která zohledňují zjištěná rizika.

Q. **Průmyslové řídicí systémy (OT)**. Společnost implementuje specifické postupy a opatření pro prostředí OT, v nichž zohledňuje komplexnost a různorodost OT a jejich odlišnosti oproti běžným informačním a komunikačním technologiím. Příslušní specialisté v oblasti řídicích systémů a telekomunikací i další zaměstnanci jsou informováni o svých úlohách a povinnostech z hlediska informační bezpečnosti v oblasti OT.

R. **Bezpečnost lidských zdrojů.** Společnost má zavedeny vhodné postupy pro všechny fáze a) před přijetím do zaměstnání (např. prověřování uchazečů) b) v průběhu zaměstnání (např. odpovědnost za řízení, školení v oblasti kybernetické bezpečnosti, disciplinární postupy) c) při ukončení, případně změně zaměstnání (zaměřené na postupy při odchodu zaměstnanců či změně jejich pozic).

S. **Dodržování právních předpisů.** Společnost uplatňuje vhodné postupy k zajištění dodržování právních předpisů zejména v oblasti Obecného nařízení o ochraně osobních údajů (GDPR) a implementace směrnice o bezpečnosti sítí a informací (NIS) ve vnitrostátním právu (právní předpisy v oblasti kybernetické bezpečnosti).

T. **Bezpečnost v rámci životního cyklu IT a OT.** Kybernetickou bezpečnost je nutné integrovat do všech fází životního cyklu systémů IT a OT, zejména v oblasti nákupu, provozu a řízení změn.

5 ZÁVĚREČNÁ USTANOVENÍ

5.1 Související interní normy a dokumenty

- Interní normy vztahující se na oblast kybernetické bezpečnosti (bezpečnostní politiky), na oblast používání výpočetní techniky, ISMS (systém řízení informační bezpečnosti), řízení změn, řízení rizik a řízení kontinuity podnikání.
- Směrnice č. 4/2018 – Zpracování osobních údajů (zejm. Informace o zpracování os. údajů)