Slovenská elektrizačná prenosová sústava	Politika	Dátum uverejnenia: 07.09.2022
	vydanie 04	Účinnosť od: dňa uverejnenia
Tento dokument ruší: -		
Číslo uznesenia: -		

Politika informačnej bezpečnosti

	Meno	Pracovná pozícia	Dátum	Podpis
Spracoval:	Ing. Miloslav Ďurčík	špecialista	26.8.2022	v. r.
Manažér procesu:	Ing. Dalibor Žiaran, MBA	VyR sekcie bezpečnosti a ISM	26.8.2022	v. r.
Overil za oblasť ISM:	Mgr. Lujza Kollerová	Vedúci odboru ISM a environmentalistiky	26.8.2022	v. r.

1. Poslanie spoločnosti SEPS

Poslaním spoločnosti Slovenská elektrizačná prenosová sústava, a.s. (ďalej len SEPS) je spoľahlivo prevádzkovať prenosovú sústavu, zabezpečovať dispečerské riadenie sústavy, jej údržbu, obnovu a rozvoj tak, aby bola zaručená spoľahlivá a kvalitná dodávka elektriny všetkým používateľom prenosovej sústavy a jej paralelná prevádzka so susednými prenosovými sústavami.

Jedným zo základných predpokladov pre dosiahnutie tohto poslania, je nevyhnutnosť zaobchádzať s údajmi a informáciami jednak priamo vo vlastníctve SEPS, ako aj s údajmi a informáciami získanými od tretích strán veľmi zodpovedne a uplatňovať pri ich používaní všetky zásady bezpečného nakladania s informáciami a údajmi, vždy v súlade s pravidlami pre daný stupeň utajenia/citlivosti týchto informácií alebo údajov.

2. Záväzok manažmentu

Vrcholový manažment spoločnosti SEPS sa touto Politikou zaväzuje, že zaistí dostupnosť všetkých potrebných zdrojov na vypracovanie, zavedenie, trvalý rozvoj a kontinuálne zlepšovanie informačnej a kybernetickej bezpečnosti v súlade s požiadavkami certifikovaného systému riadenia informačnej bezpečnosti podľa platnej verzie štandardu ISO 27001 a legislatívnych požiadaviek vyplývajúcich zo zákona o kybernetickej bezpečnosti spolu s vykonávacími vyhláškami.

3. Určenie Politiky informačnej bezpečnosti

Politika určuje hlavné ciele systému riadenia informačnej bezpečnosti budovaného a využívaného so snahou minimalizovať možnosti úniku a zneužitia citlivých informácií vyskytujúcich sa pri činnosti spoločnosti SEPS.

Politika informačnej bezpečnosti je určená a záväzná pre všetkých zamestnancov spoločnosti SEPS ako aj pre zmluvných partnerov spoločnosti.

4. Hlavné ciele systému riadenia informačnej bezpečnosti

Hlavným cieľom systému riadenia informačnej bezpečnosti je priebežne optimalizovať a zlepšovať úroveň informačnej a kybernetickej bezpečnosti a tým podporovať dosiahnutie poslania spoločnosti s dôrazom na primeranú ochranu integrity, dostupnosti a dôvernosti aktív.

Ciele systému riadenia informačnej a kybernetickej bezpečnosti sú každoročne definované v dokumente "Ciele integrovaného systému manažérstva SEPS" a podporované dokumentom "Plán zvládania rizík".

Plnenie cieľov sa vyhodnocuje priebežne a pravidelne. O výsledkoch vyhodnotenia plnenia cieľov je informované vedenie spoločnosti dokumentom "Preskúmanie ISM manažmentom".

5. Súlad Politiky informačnej bezpečnosti

Táto Politika, ako aj ostatné dokumenty systému riadenia informačnej bezpečnosti sú v súlade s právnymi a regulačnými požiadavkami SR ktoré sa týkajú spoločnosti SEPS. Týka sa to hlavne zákona o kybernetickej bezpečnosti a zákona o kritickej infraštruktúre.

Táto politika je súčasťou integrovaného systému riadenia v SEPS a to aj podľa ISO 9001 riadenie kvality, ISO 14001 riadenie ochrany životného prostredia a ISO 45001 riadenie BOZP .

6. Opatrenia informačnej bezpečnosti

Záujmy vrcholového manažmentu v SEPS pre oblasť informačnej a kybernetickej bezpečnosti zastupuje a riadi Manažér kybernetickej bezpečnosti.

Všetky opatrenia informačnej bezpečnosti sú v spoločnosti SEPS implementované v súlade a v rozsahu Prílohy A, štandardu ISO 27001. Všetky implementované opatrenia a ciele riadenia sú uvedené v dokumente "Vyhlásenie o aplikovateľnosti".

V SEPS sú všetky informácie klasifikované a používané v súlade so schválenými spôsobmi používania informácií v jednotlivých klasifikačných triedach.

Všetky zásady a opatrenia sú organizované a riadené podľa rizík informačnej a kybernetickej bezpečnosti, ktoré sa priebežne a pravidelne identifikujú, analyzujú, hodnotia a prijímajú sa k nim opatrenia, aby sa znížil ich vplyv na podnikateľskú činnosť SEPS.

Kritériá na výber a implementáciu vhodných organizačných, personálnych a technických opatrení na efektívne riadenie rizík sú súčasťou systému riadenia rizík zavedenej v spoločnosti SEPS a vychádzajú z metodiky NBÚ Metodika analýzy rizík kybernetickej bezpečnosti, z medzinárodnej technickej normy ISO/IEC ISO 27005 - Riadenie rizík a ISO 31 000 Manažérstvo rizika, Zásady a návod.

V súvislosti s riadením informačnej a kybernetickej bezpečnosti SEPS zaviedol aj proces neustáleho zlepšovania procesov informačnej a kybernetickej bezpečnosti.

Všetky uvedené opatrenia majú cieľ udržiavať zhodu s legislatívnymi požiadavkami SR na kybernetickú bezpečnosť a technickými požiadavkami na implementovanie systému riadenia informačnej bezpečnosti ISMS.

Schválil:	Ing. Peter Dovhun	26.08.2022	v. r.
	generálny riaditeľ	Dátum	Podpis