CRNOGORSKI ELEKTROPRENOSNI SISTEM AD	Tip dokumenta: Politika	Izdanje br. 2
	Ref. Br.: ISMS 009	Datum: 20.10.2021.

POLITIKA SIGURNOSTI INFORMACIJA

Opis:	Krovna politika za uspostavljanje, razvoj i unaprjeđivanje sistema za upravljanje sigurnošću informacija (ISMS)	
Izradio:	Sektor za IKT	
Ovjerio:	Sektor za regulatorne, pravne i poslove međunarodne saradnje	
Odobrio:	Izvršni direktor	Ivan Asanović, dipl. ing. el.

Primjenjuje se na: CGES

Ovaj dokument stupa na snagu danom donošenja

Usvajanjem Izdanja br.2 ove politike, prestaje da važi Izdanje br.1 ISMS 009 POLITIKE SIGURNOSTI INFORMACIJA (arh.br. 9642/6 od 18.09.2020. godine).

Ovom politikom se uspostavlja okvir za implementaciju sistema za upravljanje sigurnošću informacija – ISMS *(eng. Information Security Management System)* koji sadrži administrativne, tehničke i fizičke mjere za zaštitu podataka i informacione imovine koju koristi Crnogorski Elektroprenosni Sistem AD (u daljem tekstu: CGES) od gubitka, zloupotrebe, neovlašćenog pristupa, otkrivanja, izmjene i uništenja.

CGES ovom politikom iskazuje posvećenost rukovodstva i svih zaposlenih CGES-a stalnom povećanju stepena sigurnosti i zaštite poslovnih procesa i informacione imovine, prilikom pružanja i korišćenja usluga CGES-a. Uspostavljanje, stalni razvoj, praćenje rada i unaprjeđenje ISMS-a ima za cilj da obezbijedi integritet, raspoloživost i povjerljivost podataka i informacione imovine CGES-a, kao i da iste, uz postizanje usaglašenosti sa zakonskom regulativom, regulatornim i ugovornim zahtjevima, zaštiti od svih vrsta sigurnosnih prijetnji.

Na ovaj način, CGES preduzima preventivne mjere za sistemsku zaštitu svojih informacionih sistema. Stvaranje sigurnog okruženja, posmatrano u širem smislu, predstavlja i preduslov za participaciju CGES-a u međunarodnim i prekograničnim aktivnostima i koordinaciju sa ostalim operatorima prenosnih sistema. Politika takođe tretira oblast upravljanja informacionom bezbjednošću u skladu sa MVS sporazumom i MVS sigurnosnim planom ENTSO-e (koji se oslanja na ISO/IEC 27001:2013 standard).

Pod politikom sigurnosti informacija podrazumijeva se hijerarhijski uređen skup dokumenata koji predstavlja osnovu za implementaciju, primjenu, održavanje i unaprijeđivanje sistema upravljanja informacionom bezbjednošću u CGES-u.

Definisanje i kreiranje sigurnosnih zahtjeva odnosi se na informacione sisteme koji su u vlasništvu CGES-a, informacione sisteme trećih strana koji se privremeno ili trajno koriste u CGES-u, a obavezujuće je za sve zaposlene u CGES-u, dobavljače, izvođače i korisnike usluga CGES-a. Uz kontinuirano podizanje svijesti svih zaposlenih o značaju sigurnosti informacija, vrši se dokumentovanje svih postupaka koji podržavaju ovu politiku, uključujući i preduzete mjere za kontrolu lozinki, prava pristupa, zlonamjerni softver, fizičku sigurnost, planove održavanja kontinuiteta poslovanja i dr. Usaglašenost sa najboljom praksom u upravljanju informacionom sigurnošću i rizicima vezanim za informacionu imovinu, sprovodi se u skladu sa identifikovanim rizicima i raspoloživim resursima.

Na ovaj način se doprinosi sprječavanju pojave sigurnosnih incidenata, odnosno minimizira se njihov uticaj i šteta za poslovanje (ukoliko do njih ipak dođe) osiguravajući kontinuitet poslovanja, ali i poslovnu reputaciju CGES-a.

Sagledavajući prijetnje kako iz internog tako i eksternog okruženja, ranjivosti informacione imovine i mogućnosti eksploatacije prepoznatih ranjivosti, te ugrožavanja imovine u smislu poverljivosti, dostupnosti i integriteta, a u cilju obezbjeđivanja sigurnosti informacija u CGES-u u skladu sa poslovnim zahtjevima, relevantnim zakonima, standardima i sigurnosnim planovima energetske zajednice, ISMS politikama se definišu pravila za:

- ✓ Kontinuirano preispitivanje i unaprjeđivanje adekvatnosti i efikasnosti sistema bezbjednosti informacija;
- ✓ Bezbjednost prilikom rada sa udaljenih lokacija i korišćenja prenosivih uređaja;

- ✓ Razumijevanje odgovornosti menadžmenta, zaposlenih i trećih strana u pogledu odgovornosti za bezbjednost informacija, osposobljenosti za radne zadatke i za smanjenje rizika od krađe, prevare ili zloupotrebe opreme i informacija;
- ✓ Obezbjeđenje sigurnosti informacija u procesu zasnivanja radnog odnosa, prestanka radnog odnosa i promjene radnog mjesta;
- ✓ Identifikovanje IT imovine CGES i definisanje odgovornosti u pogledu zaštite;
- ✓ Obezbjeđenje da će informacije dobiti odgovarajući nivo zaštite, u skladu sa njihovim značajem za CGES i klasifikacijom;
- ✓ Sprječavanje neovlaštenog razotkrivanja, mijenjanja ili uništenja informacija koje se čuvaju na medijima;
- ✓ Ograničenje pristupa informacijama i opremi za obradu informacija u skladu sa poslovnim potrebama;
- ✓ Obezbjeđenje pristupa ovlašćenim korisnicima i sprječavanje neovlašćenog pristupa sistemima i uslugama;
- ✓ Podjela uloga i odgovornosti u procesu provjere vjerodostojnosti (npr lozinke, šifre, ključevi);
- ✓ Obezbjeđenje odgovarajućeg i efektivnog korišćenja kriptografije u cilju zaštite povjerljivosti, vjerodostojnosti i/ili integriteta informacija;
- ✓ Sprečavanje gubitka, oštećenja, krađe ili kompromitovanja imovine i prekida rada CGES;
- ✓ Obezbjeđenje ispravnog i bezbjednog rada sredstava za obradu informacija;
- ✓ Obezbjeđenje zaštite informacija i opreme za obradu informacija od zlonamjernog softvera;
- ✓ Zaštitu od gubitka podataka i obezbjeđenje integriteta operativnih sistema;
- ✓ Evidentiranje događaja i generisanje dokaza;
- ✓ Sprečavanje iskorištavanja tehničkih ranjivosti;
- ✓ Obezbjeđenje bezbjednosti tokom prenosa informacija unutar CGES, kao i prema spoljnim subjektima;
- ✓ Obezbjeđenje da bezbjednost informacija bude sastavni dio informacionih sistema tokom cjelokupnog životnog ciklusa;
- ✓ Obezbjeđenje zaštite imovine CGES koja je dostupna dobavljačima;
- ✓ Održavanje dogovorenog nivoa bezbjednosti informacija i pružanja usluga u skladu sa sporazumima sa dobavljačima;
- ✓ Obezbjeđenje dosljednog i efektivnog pristupa upravljanju incidentima, uključujući komunikaciju o sigurnosnim događajima i slabostima;
- ✓ Obezbjeđenje da je kontinuitet bezbjednosti informacija ugrađen u sisteme poslovanja CGES;
- ✓ Obezbjedivanje dostupnosti sredstava za obradu informacija;
- ✓ Izbjegavanje kršenja bilo kojih propisa, zakonskih, statutarnih ili ugovornih obaveza koje se odnose na bezbjednost informacija, kao i bilo kojih zahtjeva za bezbjednost;
- ✓ Obezbjeđivanje da je bezbjednost informacija funkcionalna, u skladu sa politikama i procedurama CGES.

Ova politika sigurnosti informacija predstavlja osnov za usvajanje posebnih akata u ovoj oblasti, kao i politika i procedura za pojedine segmente ISMS-a, poštujući preporuke i najbolju praksu zasnovanu na međunarodnim standardima prilikom izrade navedenih propisa.

Drugi korak u uspostavljanju ISMS-a je implementacija usvojenih politika i procedura na informacionim sistemima u poslovnom okruženju CGES-a. Struktura odgovornosti za sprovođenje ove politike je uspostavljena kroz pojedinačne akte, pravilnike, politike i procedure za ovu oblast. Koordinator informacione bezbjednosti u CGES-u djeluje kao

jedinstvena kontakt tačka (SPOC – *Single Point of Contact*) za sva pitanja vezana za informacionu bezbjednost u CGES i odgovoran je za koordinaciju primjene politika i procedura koje se odnose na informacionu bezbjednost.

Redovan nadzor, kontrola, postavljanje i preispitivanje ISMS ciljeva doprinosi bezbjednijem, efikasnijem, efektivnijem i kvalitetnijem radu CGES-a u cjelini. Ovom politikom se uspostavlja i obaveza periodičnih pregleda uspostavljenih sigurnosnih kontrola ISMS-a, kao i obaveza ad-hoc pregleda ISMS-a, odmah nakon izmjene određenih planova bezbjednosti vezanih za međunarodne sporazume, primjenu preporuka eksternih revizija ili nakon ugrožavanja bezbjednosti, sigurnosnog rizika, ili bilo kog većeg incidenta pri korišćenju podataka u CGES-u, koji su unutar opsega ovog ISMS-a.

Rukovodstvo CGES-a i svi radnici bez rezerve i u cijelosti podržavaju definisanu Politiku sigurnosti informacija, a razvoj ISMS-a u poslovnom okruženju je stalni zadatak svih zaposlenih kompanije. Poštovanje temeljnih načela Politike sigurnosti informacija postavlja se kao zahtjev kroz ugovorne obaveze CGES-a.