ATVP

Agencija za trg vrednostnih papirjev

Krovna varnostna politika

Namen dokumenta:	Opredelitev Sistema za upravljanje varovanja informacij (SUVI)		
Verzija:	**VELJAVNA 11.0**		
Stopnja zaupnosti:	**JAVNO**	**Število strani:**	**7**
			GC: 014-1/2018-127
Datum zadnje spremembe:	**07.03.2022**	**Datum odobritve:**	**07.03.2022**
Referenčni dokumenti:	**/**		
Sklici na navedene dokumente v politiki:	**Politika varnega poslovanja Agencije** **Varnostni forum** **Ocena tveganja (metodologija)** **Notranja presoja** **Vodstveni pregled** **Izjava o primernosti (SOA)** **Izvlečki varnostnih politik** **Politika fizičnega dostopa**		

Skrbnik : **Marko Vozelj**	AGENCIJA ZA TRG VREDNOSTNIH PAPIRJEV 4	Odobril/Avtoriziral: **Anka Čadež, direktorica**

1. Uvod

Agencija za trg vrednostnih papirjev (v nadaljevanju Agencija) je pravna oseba javnega prava. Pri opravljanju svojega dela je neodvisna in samostojna. Njeno temeljno poslanstvo je zagotavljanje varnega, preglednega in učinkovitega trga finančnih instrumentov.

Vizija Agencije

Agencija kot samostojna in neodvisna nadzorna institucija učinkovito izvaja nadzor nad nadzorovanimi subjekti trga finančnih instrumentov (kapitalskega trga) in zagotavlja ustrezne evropske standarde nadzora v skladu z evropskim pravnim redom in delovanjem ESME.

Strategija delovanja Agencije

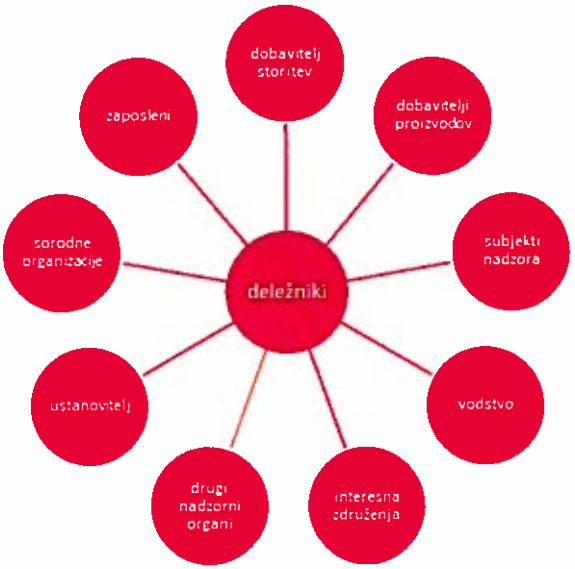
Z optimalnim izkoriščanjem kadrovskih, materialnih in finančnih virov Agencije in sodelovanjem z ostalimi sorodnimi institucijami v RS (Banka Slovenije, AZN, Ministrstvo za finance, ANR, Urad za preprečevanje pranja denarja in druga) in v EU (ESMA) skrbeti za učinkovit, urejen in ustrezno nadzorovan trg finančnih instrumentov v Republiki Sloveniji.

Cilji delovanja Agencije

1. **Krepiti zaupanje med udeleženci kapitalskega trga in investitorji**
2. **Povečati ugled in zaupanje v delovanje nadzornih institucij**
3. **Z ustreznim delovanjem zagotavljati dolgoročen uspešen razvoj trga finančnih instrumentov v Sloveniji**

Opis konteksta in obsega SUVI:

Okolje Agencije sestavljajo naslednji deležniki:



Deležniki in njihova pričakovanja glede varovanja informacij:

- **dobavitelj storitev** (pogodbe o varstvu podatkov, SUVI)
- **dobavitelji proizvodov** (pogodbe o varstvu podatkov, SUVI)
- **subjekti nadzora** (ZTFI, ZVOP, nadzorni pregledi, dostop do informacijskega sistema mora biti urejen za pridobitev licence)
- **vodstvo** (zagotavljanje virov, nadzor nad delovanjem SUVI)
- **interesna združenja** (zahteve preko interesnih združenj (podzakonski predpisi))
- **drugi nadzorni organi** skupni nadzorni organ ESMA (zahteve za poročilni sistem) – Board of Supervisors (BoS), Evropski parlament – zakonski predpisi)
- **ustanovitelj** (ZTFI in ostala zakonodaja)
- **sorodne organizacije** (AZN, ANR, BS) – posredovanje podatkov, skupni nadzori-pravilnik o medsebojnem sodelovanju nadzornih organov
- **zaposleni** (dolžnosti in odgovornosti)

2. Sistem upravljanja varovanje informacij

Osnovne naloge in pristojnosti Agencije so zlasti določene v Zakonu o trgu finančnih instrumentov, na osnovi katerega so opredeljena zunanja in notranja vprašanja, ter razumevanje potreb in pričakovanj vseh zainteresiranih strank v zvezi z varovanjem informacij.

Politika varovanja informacij izhaja iz poslanstva, vizije in strategije Agencije in določa postopke varovanja informacij v Agencije.
Postopki so skladni z zakonodajnimi določili in zahtevami standarda ISO/IEC 27001 ter zagotavljajo ustrezno:

- **zaupnost,**
- **celovitost in**
- **razpoložljivost**

informacij in informacijskega sistema za doseganje ciljev varovanja informacij, nenehno izboljševanje procesov in informacijskih sistemov Agencije.

Agencije z upoštevanjem Krovne varnostne politike in področnih varnostnih politik:

- **varuje informacije pred nepooblaščenim dostopom,**
- **ne razkriva informacij nepooblaščenim osebam,**
- **vzdržuje celovitost informacij s preprečevanjem nepooblaščenih sprememb,**
- **omogoči dostopnost do informacij pooblaščenim uporabnikom,**
- **sledi zakonskim zahtevam,**
- **ocenjuje tveganja skladno z določeno metodologijo,**
- **pripravlja, vzdržuje in preverja načrte za neprekinjeno poslovanje,**
- **zagotavlja ozaveščanje vseh zaposlenih o pomenu informacijske varnosti,**
- **beleži in poroča o vseh incidentih ter ustrezno ukrepa,**
- **zagotavlja sprejemljiv nivo informacijske varnosti ne glede na komunikacijski kanal, medij ali obliko podatkov,**
- **redno pregleduje in izboljšuje SUVI.**

S Krovno politiko varovanja informacij vodstvo Agencije izraža svojo odgovornost in zavezanost SUVI. Zaposleni in zunanji (pogodbeni) sodelavci pa z upoštevanjem postopkov potrjujejo svojo odgovornost izvajanja Krovne in področnih politik varovanja informacij.

3. Cilji krovne varnostne politike

- Zagotoviti strankam in zunanjim (pogodbenim) sodelavcem, da bomo ščitili vse informacije, ki jih od njih pridobimo oz. nastanejo v procesu sodelovanja z njimi.
- Nadzorovati informacijski sistem ter oceniti morebitna tveganja, ki lahko ogrozijo informacije.
- Upravljati s tveganji in le-ta znižati na sprejemljiv nivo.
- Zagotoviti kibernetsko varnost in na podatkih osnovano organizacijo
- Vzdrževati certifikacijo SUVI po veljavnem standardu ISO/IEC 27001.

4. Področje veljavnosti

Sistem upravljanja varovanja informacij obsega celotno poslovanje Agencije v prostorih, ki so opredeljeni v Politiki fizičnega dostopa.

Agencija omogoča tudi delo od doma, po vnaprej določenem protokolu v skladu s Pravilnikom o delu na domu in zato področje veljavnosti SUVI smiselno obsega tudi prostore na domu zaposlenih in zaposlene, ki delajo od doma.

5. Dokumentacija SUVI

Politika varovanja informacij v Agenciji kot del SUVI vključuje postopke varovanja informacij, ki so predstavljeni v 14. področjih varovanja informacij ter so skladni s cilji politike.

1) **Varnostne politike**
   Cilj: Zagotoviti usmeritev in podporo vodstva za varovanje informacij v skladu s poslovnimi zahtevami ter področno zakonodajo in predpisi.

2) **Organiziranost varovanja informacij**

[1] Poslovnik Agencije za trg vrednostnih papirjev, Pravilnik o delu Sveta Agencije za trg vrednostnih papirjev, Pravilnik o notranji organizaciji in sistemizaciji delovnih mest, Pravilnik o varovanju zaupnih informacij Agencije za trg vrednostnih papirjev, Pravilnik o ravnanju z dokumentarnim gradivom in o hranjenju dokumentarnega gradiva, Pravilnik o določitvi delovnega časa, Navodilo za evidentiranje delovnega časa, Pravilnik o vsebini in načinu vodenja odnosov z javnostmi, Pravilnik o postopku za objavljanje informacij na spletnih straneh Agencije za trg vrednostnih papirjev.

Cilj: Oblikovati okvirni načrt, po katerem se vpelje in nadzoruje varovanje informacij v Agenciji.

3) **Varovanje v zvezi z osebjem**
Cilj: Zagotoviti, da se zaposlenim in zunanjim (pogodbenim) sodelavcem predstavi dolžnosti varovanja informacij.

4) **Upravljanje sredstev**
Cilj: Doseči in vzdrževati ustrezno varovanje sredstev Agencije.

5) **Nadzor dostopa**
Cilj: Omejiti dostop do podatkov in zmogljivosti za obdelavo podatkov.

6) **Kriptografija**
Cilj: Zagotoviti pravilno in učinkovito uporabo kriptografije za varovanje zaupnosti, celovitosti in avtentičnosti podatkov.

7) **Fizična zaščita in varovanje pred grožnjami okolja**
Cilj: Preprečiti nepooblaščen fizični dostop, škodo in motnje pri dostopu do podatkov in zmogljivosti za obdelavo podatkov.

8) **Varovanje delovanja informacijskih sistemov**
Cilj: Zagotoviti pravilno in varno delovanje zmogljivosti za obdelavo podatkov.

9) **Varovanje komunikacij**
Cilj: Zagotoviti zaščito informacij, omrežij in podpornih zmogljivosti za obdelavo informacij

10) **Nabava, razvoj in vzdrževanje informacijskih sistemov**
Cilj: Zagotoviti, da je varovanje informacij vključeno v celoten življenjski cikel informacijskih sistemov.

11) **Odnosi z dobavitelji**
Cilj: Zagotoviti zaščito podatkov, ki so dostopni dobaviteljem Agencije.

12) **Upravljanje incidentov pri varovanju informacij**
Cilj: Zagotoviti dosleden in učinkovit pristop pri upravljanju incidentov, dogodkov in slabosti pri varovanju informacij.

13) **Vidiki varovanja informacij pri upravljanju neprekinjenega poslovanja**
Cilj: Vključiti neprekinjenost varovanja informacij v upravljanje neprekinjenega poslovanja.

14) **Usklajenost**
Cilj: Zagotoviti vključenost in obvladovanje varovanje informacij v skladu s politikami in postopki ter zakonodajnimi določili.

6. Odgovornosti

Direktor Agencije je odgovoren za nadzor SUVI ter za spremljanje in nadziranje učinkovitosti postopkov varovanja informacij in informacijskega sistema ter za zagotovitev potrebnih finančnih in človeških virov.

Za delovanje SUVI je določen skrbnik SUVI (pooblaščena oseba SUVI), ki določa in izvaja naloge varovanja informacij in informacijskega sistema.

Naloge skrbnika SUVI so:

- nadziranje in zaščita dokumentov politike varovanja informacij in postopkov pri spremembah dokumentacije,
- obdobno ocenjevanje varnostnih tveganj,
- priprava načrta za obravnavo tveganj,
- izvedba notranjih presoj,
- zagotavljanje ozaveščenosti zaposlenih ter zunanjih (pogodbenih) sodelavcev,
- upravljanje z varnostnimi dogodki ali incidenti,
- izvedba varnostnih ukrepov, ki zagotavljajo primerno izvajanje politike varovanja informacij.

Delo skrbnika SUVI nadzirajo člani Varnostnega foruma.

Naloge Varnostnega foruma so:

- zagotavljanje virov in potrjevanje ukrepov, ki zagotavljajo primerno izvajanje postopkov varovanje informacij skladno z zakonodajo s področja varovanja podatkov, ob pojavu novih groženj, novih varnostnih dogodkov ali incidentov ter spremembah organizacijske ali tehnične infrastrukture,
- potrjevanje dokumentacije SUVI,
- izvedba sestankov Varnostnega foruma in vodstvenega pregleda.

7. Odgovornosti pri poročanju incidentov in varnostnih pomanjkljivosti

V proces stalnega izboljševanja postopkov varovanja informacij in informacijskega sistema so vključeni zaposleni ter zunanji (pogodbeni) sodelavci. Skrbnik SUVI ustrezno seznanja s postopki, zaposleni in zunanji (pogodbeni) sodelavci pa so dolžni sporočiti opažene varnostne dogodke ali incidente, kot so:

- pomanjkljivo izvajanje postopkov varovanja informacij in informacijskega sistema,
- nepravilno ali sumljivo delovanje informacijskih sistemov,
- nedelovanje informacijskih sistem-ov
- sum oziroma zaznava kibernetskega napada, odtujitve ali izgube podatkov
- kršitve določil SUVI.

Skrbnik SUVI zbira prijave varnostnih dogodkov ali incidentov, jih pregleduje in analizira, obvesti Varnostni forum in na incidente odgovori z ustreznimi ukrepi. O incidentih in ukrepih se vodi zapise ter se jih predstavi na sestankih Varnostnega foruma in vodstvenem pregledu.

8. Vzdrževanje SUVI

Ob spremembah zakonodaje s področja varovanja podatkov, pojavu novih groženj, novih varnostnih dogodkov ali incidentov, spremembah organizacijske ali tehnične infrastrukture, ki vplivajo na varovanje informacij in informacijskih sistemov, se SUVI nenehno prilagaja s pripravo novih in dopolnjevanjem že obstoječih postopkov varovanja informacij in

informacijskih sistemov. S tem je zagotovljeno dinamično prilagajanje politike varovanja informacij v skladu z zahtevami in spremembami, ki se bodo odvijale v Agenciji.

9. Upravljanje z dokumenti politike varovanja informacij

Dokumenti politike varovanja informacij so objavljeni na intranetu Agencije tako, da so dostopni zaposlenim in zunanjim (pogodbenim) sodelavcem, ki jih morajo upoštevati pri svojem delu.

10. Sankcije

Vsako neupoštevanje določil zahtev varovanja informacij in pripadajočih dokumentov, ki pomembnejše vpliva na delovanje Agencije, se šteje za kršitev pogodbe o delu ali pogodbe o sodelovanju in se kot tako tudi sankcionira.