Povzetek Splošnih varnostnih politik Zavarovalne skupine Sava

Ljubljana, april 2025

Kazalo

1 UVOD

Ta dokument povzema ključne splošne varnostne politike Zavarovalne skupine Sava (v nadaljevanju ZSS), prilagojene za javno objavo za potrebe dobaviteljev. Namenjen je vsem pogodbenim partnerjem, ki pri svojem delu in za izvajanje pogodbenih storitev dostopajo do kakršnih koli IKT-virov ZSS (npr. aplikacije, telekomunikacijska sredstva, podatkovne zbirke idr.) ali jih uporabljajo.

Ta povzetek obsega naslednje vsebine:

- pravilna uporaba vseh informacijskih virov oziroma IKT-virov,
- upravljanje informacijskih virov oziroma IKT-virov,
- elektronsko poslovanje,
- varovanje opreme in informacijskih virov oziroma IKT-virov.

S sprejetjem Splošnih varnostnih politik ZSS se dobavitelj (pogodbeni partner) zavezuje, da bo pri izvajanju pogodbenih obveznosti spoštoval varnostne zahteve informacijske tehnologije v skladu z veljavnimi dobrimi praksami, minimalnimi standardi in načeli stroke ter veljavnimi predpisi.

2 NAMEN IN OBSEG VARNOSTNIH POLITIK

Namen varnostnih politik v ZSS je:

- zagotovitev varne in primerne uporabe IKT-virov,
- seznanitev uporabnikov s tveganji, povezanimi z uporabo IKT-virov,
- opredelitev ukrepov za zaščito informacij pred nepooblaščenim razkritjem ali zlorabo.

Pogodbeni uporabniki morajo vse IKT-vire ZSS uporabljati vestno, učinkovito in odgovorno.

ZSS v najvišji možni meri varuje zaposlene in svojo lastnino pred nezakonitimi ali škodljivimi namernimi ali nenamernimi aktivnostmi posameznikov.

Neustrezna uporaba informacijske tehnologije izpostavlja ZSS in njene uporabnike tveganjem, kot so okužbe informacijske tehnologije z računalniškimi virusi, ogrožanje omrežnih sistemov in storitev ter zloraba informacij in podatkov, shranjenih v informacijskem sistemu ZSS.

3 SPLOŠNE ZAHTEVE

- Dobavitelj mora upoštevati vse veljavne zakone in predpise, vključno s Splošno uredbo o varstvu podatkov (GDPR) in Uredbo o digitalni operativni odpornosti za finančni sektor (DORA).
- Dobavitelj mora imenovati kontaktno osebo za varnostne komunikacije in odziv na incidente.

4 UPRAVLJANJE DOSTOPA

- Dobavitelj mora vzpostaviti stroge kontrole za preprečevanje dostopa do IKT-sistemov ZSS nepooblaščenim osebam.
- Dobavitelj mora vzpostaviti stroge kontrole, s čimer zagotovi, da do IKT-sistemov ZSS dostopajo le pooblaščene osebe, ki so ustrezno preverjene in usposobljene.
- Upravljanje dostopov se nanaša na vse oblike dostopa do IKT-virov, ki med drugim vključujejo:
    - uporabniške dostope prek uporabniških vmesnikov (GUI),
    - dostope prek programskih vmesnikov (API),
    - sistemske/storitvene dostope (servisni računi),
    - administratorske in privilegirane dostope,

  - skripte, časovna opravila (angl. cron job) in avtomatizirane integracije,
  - oddaljene dostope (VPN, RDP, SSH idr.),
  - dostope prek mobilnih naprav ali oblaka.
- Zaščita dostopov do IKT-sistemov ZSS med drugim vključuje večfaktorsko avtentikacijo (MFA) in uporabo načela najmanjšega privilegija (angl. least privilege).
- Vsi dostopi do sistemov ali podatkov, povezanih z ZSS, se zaradi zagotavljanja revizijske sledi zabeležijo in spremljajo.
- Dobavitelj mora vzdrževati posodobljen seznam pooblaščenega osebja z dostopnimi pravicami do IKT-sistemov ZSS in ga redno pregledovati.

5 ZAŠČITA PODATKOV

- Dobavitelj mora zagotoviti celovitost, zaupnost in razpoložljivost podatkov.
- Vsi podatki med prenosom morajo biti šifrirani z uporabo kriptografskega protokola TLS 1.2 ali novejše različice.
- Vsi podatki v mirovanju, vključno z varnostnimi kopijami, morajo biti šifrirani z uporabo standarda AES-256 ali enakovrednega standarda.
- Dobavitelj mora zagotoviti, da so delovni računalniki, ki se uporabljajo za izvajanje pogodbene storitve, redno varnostno posodobljeni, imajo nameščeno izključno zakonito programsko opremo in so zaščiteni z redno posodobljenim protivirusnim sistemom.
- Dobavitelj mora zagotoviti minimizacijo obdelave in shranjevanja podatkov, pri čemer sme obdelovati in shranjevati le tiste podatke, ki so nujno potrebni za izvedbo pogodbenih obveznosti.
- Dobavitelj se mora izogibati nepotrebnemu shranjevanju podatkov in zagotoviti, da se podatki brišejo ali anonimizirajo takoj po prenehanju potrebe po shranjevanju.
- Dobavitelj mora ob prenehanju pogodbenega razmerja podatke varno izbrisati ali v celoti vrniti ZSS.

6 UPRAVLJANJE INCIDENTOV

- Dobavitelj mora imeti politiko upravljanja incidentov, ki vključuje odkrivanje, sporočanje in reševanje varnostnih incidentov.
- Varnostni incidenti dobavitelja, ki vplivajo na ZSS, morajo biti ZSS prijavljeni v 24 urah.
- Dobavitelj mora ZSS omogočiti sodelovanje pri reševanju incidenta, ki ima vpliv na njen IKT-sistem, vključno z zagotavljanjem dostopa do ustrezne dokumentacije.

7 ODPORNOST IN KONTINUITETA

- Dobavitelj mora imeti vzpostavljen načrt za neprekinjeno poslovanje (angl. Business Continuity Plan – BCP) in načrt za odzivanje na katastrofe (angl. Disaster Recovery Plan – DRP), ki vključujeta periodično testiranje.
- Načrte je treba letno preizkusiti, rezultate pa deliti z ZSS na zahtevo.

8 UPRAVLJANJE PODIZVAJALCEV, POVEZANIH S POGODBENO STORITVIJO

- Dobavitelj mora pridobiti pisno soglasje naročnika (ZSS) pred vključitvijo podizvajalcev ali tretjih oseb.
- Dobavitelj mora zagotoviti, da vsi podizvajalci izpolnjujejo enake zahteve, kot bi jih moral sam.

9 REVIZIJA IN OCENJEVANJE TVEGANJ

- Dobavitelj mora izvajati redne ocene tveganj, povezanih s svojimi storitvami, in vključiti naročnika (ZSS) v ocenjevanje, kjer je to primerno.
- Naročnik (ZSS) o dobavitelju pripravi lastno oceno tveganja, kar lahko vključuje posredovanje varnostnih vprašalnikov dobavitelju in izvedbo neodvisnih pregledov varnostnih ukrepov.
- Dobavitelj mora na zahtevo naročnika predložiti poročila o svojih revizijah in testiranjih, posredovati odgovore na varnostne vprašalnike in razumno sodelovati pri izvedbi neodvisnih pregledov.
- Naročnik (ZSS) ima pravico do rednih revizij in neodvisnih pregledov varnostnih ukrepov dobavitelja.
- Dobavitelj mora na zahtevo ZSS predložiti dokaze o skladnosti, kot so certifikati, poročila ali rezultati v zvezi z varnostnimi testi.

10 IZOBRAŽEVANJE IN OZAVEŠČANJE

- Dobavitelj mora redno usposabljati svoje zaposlene, ki delajo za naročnika (ZSS), o dobrih praksah informacijske varnosti in drugih vsebinah, če to zahteva naročnik (ZSS).

11 PRENEHANJE SODELOVANJA

- Po prenehanju pogodbe mora dobavitelj zagotoviti varen izklop storitev iz IKT-sistema ZSS, vključno z ukinitvijo dostopov in varnim izbrisom vseh podatkov ZSS.
- Po prenehanju pogodbe mora dobavitelj predložiti izjavo ali drugo dokazilo o izbrisu podatkov.

12 POSODOBITVE IN SPREMEMBE

- ZSS si pridržuje pravico, da posodobi ta dokument, s čimer se zagotovi odziv na spremembe tveganj, tehnologije ali predpisov. Dobavitelj bo o posodobitvah obveščen in bo moral v razumnem času zagotoviti skladnost.

13 POJMI IN KRATICE

Št.	Pojem/kratica	Opis
3	**ZSS**	Zavarovalna skupina Sava
4	**IKT**	Informacijsko-komunikacijska tehnologija – tehnologija, ki omogoča zbiranje, obdelavo in izmenjavo podatkov
5	**MFA**	Multi-Factor Authentication – večstopenjska avtentikacija za povečanje varnosti dostopa
7	**AES-256**	Advanced Encryption Standard (256-bit) – kriptografski šifrirni algoritem za zaščito podatkov v mirovanju
8	**TLS 1.2**	Transport Layer Security 1.2 – kriptografski protokol za varno komunikacijo v omrežjih