Sažetak Opštih bezbednosnih politika Osiguravajuće grupe Sava

Ljubljana, april 2025

Sadržaj

1 UVOD

Ovaj dokument sažima ključne opšte bezbednosne politike Osiguravajuće grupe Sava (u daljem tekstu: ZSS), prilagođene za javnu objavu u svrhu informisanja Dobavljača. Namenjen je svim ugovornim partnerima koji u okviru svog posla i za izvršavanje ugovornih usluga pristupaju bilo kojim IKT-resursima OGS-a (npr. aplikacijama, telekomunikacionim sredstvima, bazama podataka itd.) ili ih koriste.

Ovaj sažetak obuhvata sledeće oblasti:

- pravilna upotreba svih informacionih, odnosno IKT-resursa,
- upravljanje informacioninim resursima, odnosno IKT resursima,
- elektronsko poslovanje,
- zaštita opreme i informacionih resursa, odnosno IKT resursa.

Prihvatanjem Opštih bezbednosnih politika ZZS-a, Dobavljač (ugovorni partner) se obavezuje da će prilikom izvršavanja ugovornih obaveza poštovati zahteve informacione bezbednosti u skladu sa važećim dobrim praksama, minimalnim standardima, stručnim načelima i važećim propisima.

2 SVRHA I OBIM BEZBEDNOSNIH POLITIKA

Svrha bezbednosnih politika u ZSS-u je:

- obezbeđivanje bezbednog i odgovarajućeg korišćenja IKT - resursa,
- informisanje korisnika o rizicima povezanim sa korišćenjem IKT - resursa,
- definisanje mera zaštite informacija od neovlašćenog otkrivanja ili zloupotrebe.

Ugovorni korisnici moraju koristiti sve IKT-resurse OGS-a savesno, efikasno i odgovorno.

ZSS u najvećoj mogućoj meri štiti zaposlene i svoju imovinu od nezakonitih ili štetnih aktivnosti pojedinaca, bile one namerne ili nenamerne.

Neadekvatna upotreba informacionih tehnologija izlaže ZSS i njegove korisnike rizicima kao što su napadi na informacione tehnologije računarskim virusima, ugrožavanje mrežnih sistema i usluga, kao i zloupotreba informacija i podataka koji se čuvaju u informacionom sistemu ZSS-a.

3 OPŠTI ZAHTEVI

- Dobavljač mora poštovati sve važeće zakone i propise, uključujući Opštu uredbu o zaštiti podataka (GDPR) i Uredbu o digitalnoj operativnoj otpornosti za finansijski sektor (DORA).
- Dobavljač mora imenovati kontakt osobu za bezbednosnu komunikaciju i reagovanje na incidente.

4 UPRAVLJANJE PRISTUPOM

- Dobavljač mora uspostaviti stroge kontrole kako bi sprečio pristup IKT-sistemima OGS-a neovlašćenim licima.
- Dobavljač mora uspostaviti stroge kontrole kako bi osigurao da pristup IKT-sistemima ZSS-a imaju isključivo ovlašćena, proverena i obučena lica.
- Upravljanje pristupom odnosi se na sve oblike pristupa IKT-resursima, uključujući:
    - korisnički pristup preko grafičkog interfejsa (GUI),
    - pristup putem programskih interfejsa (API),

  - sistemski/servisni pristup (servisni nalozi),
  - administratorski i privilegovani pristup,
  - skripte, zakazana izvršavanja (engl. cron job) i automatizovane integracije,
  - daljinski pristup (VPN, RDP, SSH itd.),
  - pristup preko mobilnih uređaja ili oblaka.
- Zaštita pristupa uključuje višefaktorsku autentifikaciju (MFA) i primenu principa najmanjih privilegija (least privilege).
- Svi pristupi sistemima ili podacima povezanima sa ZSS-om se beleže i nadgledaju zbog obezbeđivanja revizionog traga.
- Dobavljač mora održavati listu ovlašćenog osoblja ažuriranu sa pristupnim pravima za IKT-sisteme ZSS-a i redovno je pregledavati.

5 ZAŠTITA PODATAKA

- Dobavljač mora obezbediti integritet, poverljivost i dostupnost podataka.
- Svi podaci u prenosu moraju biti šifrovani korišćenjem TLS 1.2 protokola ili novije verzije.
- Svi podaci u mirovanju, uključujući rezervne kopije, moraju biti šifrovani korišćenjem AES-256 standarda ili njegovog ekvivalenta.
- Dobavljač mora obezbediti da su radni računari, koji se koriste za izvršavanje ugovorene usluge, redovno bezbednosno ažurirani, da imaju instaliran isključivo legalan softver i da su zaštićeni redovno ažuriranim antivirusnim sistemom.
- Dobavljač mora obezbediti minimizaciju obrade i skladištenja podataka, pri čemu sme obrađivati i skladištiti samo one podatke koji su neophodni za izvršenje ugovornih obaveza.
- Dobavljač mora izbegavati nepotrebno čuvanje podataka i obezbediti da se podaci brišu ili anonimizuju odmah po prestanku potrebe za njihovim čuvanjem.
- Dobavljač je u obavezi da po isteku ugovornog odnosa podatke bezbedno izbriše ili u celosti vrati ZSS-u.

6 UPRAVLJANJE INCIDENTIMA

- Dobavljač mora imati usvojenu politiku upravljanja incidentima koja obuhvata otkrivanje, prijavljivanje i rešavanje bezbednosnih incidenata.
- Bezbednosni incidenti Dobavljača koji utiču na ZSS moraju biti prijavljeni ZSS-u u roku od 24 sata.
- Dobavljač mora omogućiti ZSS-u učešće u rešavanju incidenta koji utiče na njegov IKT-sistem, uključujući obezbeđivanje pristupa relevantnoj dokumentaciji.

7 OTPORNOST I KONTINUITET

- Dobavljač mora imati uspostavljen plan za neprekidno poslovanje (engl. Business Continuity Plan – BCP) i plan za oporavak od katastrofa (engl. Disaster Recovery Plan – DRP), koji uključuju periodično testiranje.
- Planove je potrebno testirati jednom godišnje, a rezultate dostaviti ZSS-u na zahtev.

8 UPRAVLJANJE PODIZVOĐAČIMA POVEZANIM SA UGOVORENOM USLUGOM

- Dobavljač mora pribaviti pisanu saglasnost naručioca (ZSS) pre uključivanja podizvođača ili trećih lica.
- Dobavljač mora obezbediti da svi podizvođači ispunjavaju iste zahteve kao i on sam.

9 REVIZIJA I PROCENA RIZIKA

- Dobavljač mora sprovoditi redovne procene rizika povezane sa svojim uslugama i uključiti naručioca (ZSS) u proces procene, kada je to primereno.
- Naručilac (ZSS) sprovodi sopstvenu procenu rizika o Dobavljaču, što može uključivati slanje bezbednosnih upitnika i sprovođenje nezavisnih pregleda bezbednosnih mera.
- Dobavljač je dužan da na zahtev naručioca dostavi izveštaje o sprovedenim revizijama i testiranjima, odgovori na bezbednosne upitnike i razumno sarađuje pri sprovođenju nezavisnih provera.
- Naručilac (ZSS) ima pravo na redovne revizije i nezavisne provere bezbednosnih mera koje Dobavljač primenjuje.
- Dobavljač mora na zahtev ZSS-a dostaviti dokaze o usklađenosti, kao što su sertifikati, izveštaji ili rezultati bezbednosnih testova.

10 OBRAZOVANJE I PODIZANJA SVESTI

- Dobavljač je dužan da redovno obučava svoje zaposlene koji rade za naručioca (ZSS) o dobrim praksama informacione bezbednosti i drugim temama, ukoliko to zahteva naručilac (ZSS).

11 PRESTANAK SARADNJE

- Po prestanku ugovora, Dobavljač mora osigurati bezbedno isključenje usluga iz IKT-sistema ZSS-a, uključujući ukidanje pristupa i bezbedno brisanje svih podataka ZSS-a.
- Po prestanku ugovora, Dobavljač mora dostaviti izjavu ili drugi dokaz o brisanju podataka.

12 AŽURIRANJA I IZMENE

- ZSS zadržava pravo da ažurira ovaj dokument kako bi obezbedio odgovaranje na promene rizika, tehnologije ili propisa. Dobavljač će biti obavešten o izmenama i mora u razumnom roku obezbediti usklađenost.

13 POJMOVI I SKRAĆENICE

Br.	Pojam/skraćenica	Opis
3	**ZSS**	Osiguravajuća grupa Sava
4	**IKT**	Informaciono-komunikacione tehnologije – tehnologije koje omogućavaju prikupljanje, obradu i razmenu podataka
5	**MFA**	Multi-Factor Authentication – višestepena autentifikacija za povećanje bezbednosti pristupa
7	**AES-256**	Advanced Encryption Standard (256-bit) – kriptografski algoritam za zaštitu podataka u mirovanju
8	**TLS 1.2**	Transport Layer Security 1.2 – kriptografski protokol za bezbednu komunikaciju u mrežama