Sažetak općih sigurnosnih politika Osiguratelјne grupe Sava

Ljubljana, travanj 2025.

Sadržaj

1 UVOD

U ovom dokumentu sažeto se navode opće sigurnosne politike Osigurateljne grupe Sava (dalje u tekstu „OGS"), prilagođene za javnu objavu za potrebe dobavljača. Namijenjen je svim ugovornim partnerima koji pristupaju resursima IKT-a grupe OGS (npr. aplikacije, telekomunikacijska sredstva, baze podataka itd.) ili ih upotrebljavaju u svojem radu i za potrebe pružanja ugovornih usluga.

U ovom sažetku obrađuju se sljedeće teme:

- pravilna upotreba svih izvora informacija ili resursa IKT-a
- upravljanje izvorima informacija ili resursima IKT-a
- elektroničko poslovanje
- zaštita opreme i izvora informacija ili resursa IKT-a.

Prihvaćanjem Općih sigurnosnih politika grupe OGS dobavljač (ugovorni partner) obvezuje se da će pri izvršavanju ugovornih obveza poštovati sigurnosne zahtjeve informacijske tehnologije u skladu s važećim najboljim praksama, minimalnim standardima i načelima struke te važećim propisima.

2 SVRHA I PODRUČJE PRIMJENE SIGURNOSNIH POLITIKA

Svrha sigurnosnih politika grupe OGS uključuje:

- osiguravanje sigurne i odgovarajuće upotrebe resursa IKT-a
- upoznavanje korisnika s rizicima povezanima s upotrebom resursa IKT-a
- utvrđivanje mjera za zaštitu informacija od neovlaštenog otkrivanja ili zlouporabe.

Ugovorni korisnici moraju savjesno, učinkovito i odgovorno upotrebljavati sve resurse IKT-a grupe OGS.

Grupa OGS u najvećoj mogućoj mjeri štiti zaposlenike i svoju imovinu od nezakonitih ili štetnih namjernih ili nenamjernih radnji pojedinaca.

Neodgovarajuća upotreba informacijske tehnologije izlaže grupu OGS i njezine korisnike rizicima kao što je zaraza informacijske tehnologije računalnim virusima, prijetnje mrežnim sustavima i uslugama te zlouporaba informacija i podataka pohranjenih u informacijskom sustavu grupe OGS.

3 OPĆI ZAHTJEVI

- Dobavljač mora poštovati sve važeće zakone i propise, uključujući Opću uredbu o zaštiti podataka (OUZP) i Uredbu o digitalnoj operativnoj otpornosti za financijski sektor (DORA).
- Dobavljač mora imenovati osobu za kontakt za sigurnosnu komunikaciju i odgovor na incidente.

4 UPRAVLJANJE PRISTUPOM

- Dobavljač mora uvesti stroge kontrole kako bi onemogućio neovlaštenim osobama pristup sustavima IKT-a grupe OGS.
- Dobavljač mora uvesti stroge kontrole kako bi se pobrinuo da pristup sustavima IKT-a grupe OGS imaju samo propisno provjerene i osposobljene ovlaštene osobe.
- Upravljanje pristupom odnosi se na sve oblike pristupa resursima IKT-a, uključujući, među ostalim:
    - korisničke pristupe putem grafičkog korisničkog sučelja (GUI)
    - pristupe putem sučelja za programiranje aplikacija (API)

  - pristupe sustavu/uslugama (računi usluga)
  - administratorske i povlaštene pristupe
  - skripte, vremenski dodijeljene zadatke (engl. *cron*) i automatizirane integracije
  - udaljene pristupe (VPN, RDP, SSH itd.)
  - pristupe putem mobilnih uređaja ili oblaka.
- Zaštita pristupa sustavima IKT-a grupe OGS uključuje, među ostalim, višefaktorsku autentifikaciju (MFA) i primjenu načela najmanjih povlastica (engl. *least privilege*).
- Svaki pristup sustavima ili podacima povezanima s grupom OGS bilježi se i nadzire radi revizijskog traga.
- Dobavljač mora voditi i redovito pregledavati ažurirani popis ovlaštenog osoblja s pravima pristupa sustavima IKT-a grupe OGS.

5 ZAŠTITA PODATAKA

- Dobavljač mora zajamčiti cjelovitost, povjerljivost i dostupnost podataka.
- Svi podaci tijekom prijenosa moraju biti šifrirani kriptografskim protokolom TLS 1.2 ili novijom verzijom.
- Svi podaci u mirovanju, uključujući sigurnosne kopije, moraju biti šifrirani standardom AES-256 ili jednakovrijednim standardom.
- Dobavljač se mora pobrinuti da se radna računala koja se upotrebljavaju za pružanje ugovorene usluge redovito sigurnosno ažuriraju, da je na njima instaliran samo legalni softver te da su zaštićena antivirusnim sustavom koji se redovito ažurira.
- Dobavljač obradu i pohranu podataka mora svesti na najmanju moguću mjeru, pri čemu smije obrađivati i pohranjivati samo one podatke koji su nužni za izvršavanje ugovornih obveza.
- Dobavljač mora izbjegavati nepotrebnu pohranu podataka, a podatke mora izbrisati ili anonimizirati čim prestane potreba za pohranom.
- Nakon prestanka ugovornog odnosa dobavljač podatke mora na siguran način izbrisati ili u cijelosti vratiti grupi OGS.

6 UPRAVLJANJE INCIDENTIMA

- Dobavljač mora imati politiku upravljanja incidentima, koja uključuje otkrivanje, prijavljivanje i rješavanje sigurnosnih incidenata.
- Sigurnosni incidenti dobavljača koji utječu na grupu OGS moraju se prijaviti grupi OGS u roku od 24 sata.
- Dobavljač grupi OGS mora omogućiti sudjelovanje u rješavanju incidenta koji utječe na njezin sustav IKT-a, među ostalim omogućivanjem pristupa relevantnoj dokumentaciji.

7 OTPORNOST I KONTINUITET

- Dobavljač mora imati utvrđen plan kontinuiteta poslovanja (engl. *Business Continuity Plan* – BCP) i plan oporavka u slučaju katastrofe (engl. *Disaster Recovery Plan* – DRP), koji uključuju periodično testiranje.
- Te bi planove trebalo testirati svake godine, a rezultate testiranja na zahtjev podijeliti s grupom OGS.

8 UPRAVLJANJE PODIZVOĐAČIMA POVEZANIMA S UGOVORENOM USLUGOM

- Dobavljač prije uključivanja podizvođača ili trećih osoba mora dobiti pisanu suglasnost naručitelja (grupa OGS).

- Dobavljač se mora pobrinuti da svi podizvođači ispunjavaju iste zahtjeve koje bi i on sâm morao ispuniti.

9 REVIZIJA I PROCJENA RIZIKA

- Dobavljač mora provoditi redovite procjene rizika povezanih sa svojim uslugama i prema potrebi u te procjene uključiti naručitelja (grupa OGS).
- Naručitelj (grupa OGS) provodi vlastitu procjenu rizika dobavljača, koja može uključivati prosljeđivanje sigurnosnih upitnika dobavljaču i provođenje neovisnih pregleda sigurnosnih mjera.
- Na zahtjev naručitelja dobavljač mora dostaviti izvješća o svojim revizijama i testiranjima, odgovoriti na sigurnosne upitnike i u razumnoj mjeri surađivati u provođenju neovisnih pregleda.
- Naručitelj (grupa OGS) ima pravo provoditi redovite revizije i neovisne preglede sigurnosnih mjera dobavljača.
- Na zahtjev grupe OGS dobavljač mora dostaviti dokaze o sukladnosti, kao što su potvrde, izvješća ili rezultati koji se odnose na ispitivanja sigurnosti.

10 OBRAZOVANJE I INFORMIRANJE

- Dobavljač mora redovito osposobljavati svoje zaposlenike koji rade za naručitelja (grupa OGS) o dobrim praksama informacijske sigurnosti i drugim sadržajima ako to naručitelj (grupa OGS) zatraži.

11 PREKID SURADNJE

- Nakon raskida ugovora dobavljač na siguran način mora prestati s korištenjem usluga sustava IKT-a grupe OGS, uključujući ukidanje pristupa i sigurno brisanje svih podataka grupe OGS.
- Nakon raskida ugovora dobavljač mora dostaviti izjavu ili drugi dokaz o brisanju podataka.

12 AŽURIRANJA I IZMJENE

- Grupa OGS zadržava pravo ažuriranja ovog dokumenta kako bi on bio u skladu s promjenama rizika, tehnologije ili propisa. Dobavljač će biti obaviješten o tim ažuriranjima te će se u razumnom roku s njima morati uskladiti.

13 POJMOVI I POKRATE

Br.	Pojam/pokrata	Opis
3	**OGS**	Osigurateljna grupa Sava
4	**IKT**	Informacijska i komunikacijska tehnologija – tehnologija koja omogućuje prikupljanje, obradu i razmjenu podataka
5	**MFA**	*Multi-Factor Authentication* – višefaktorska autentifikacija radi poboljšanja sigurnosti pristupa
7	**AES-256**	*Advanced Encryption Standard (256-bit)* – algoritam kriptografskog šifriranja za zaštitu podataka u mirovanju
8	**TLS 1.2**	*Transport Layer Security 1.2* – kriptografski protokol za sigurnu komunikaciju u mrežama