Informacion kyç
nga Politikat e Përgjithshme të Sigurisë të Sava Insurance Group

Lubjanë, prill 2025

Përmbajtja

1 HYRJE

Ky dokument përmbledh politikat kryesore të përgjithshme të sigurisë të Sava Insurance Group (SIG), të përshtatura për deklarim publik për qëllime në lidhje me ofruesit. Synohet për të gjithë partnerët kontraktualë të cilët, në kohëzgjatjen e punës së tyre dhe të performancës së shërbimeve kontraktuale, kanë akses ose përdorin ndonjë nga burimet e SIG ICT (p.sh. aplikacione, mënyra telekomunikimi, baza të dhënash etj.).

Kjo përmbledhje përfshin përmbajtjen e mëposhtme:

- përdorimin e duhur të të gjithë informacionit ose të burimeve ICT,
- menaxhimin e informacionit ose të burimeve ICT,
- operacionet elektronike,
- mbrojtjen e pajisjeve dhe informacionit ose të burimeve ICT.

Duke pranuar Politikat e Përgjithshme të Sigurisë të SIG, ofruesi (partneri kontraktual) merr përsipër të pajtohet me kërkesat e sigurisë të IT sipas praktikave më të mira të zbatueshme, standardet minimale dhe parimet profesionale, si edhe me rregulloret e zbatueshme gjatë përmbushjes së detyrimeve të veta kontraktuale.

2 QËLLIMI DHE SHTRIRJA E POLITIKAVE TË SIGURISË

Qëllimi i politikave të sigurisë të SIG është:

- të garantojë përdorimin e sigurt dhe të përshtatshëm të burimeve ICT,
- të njohë përdoruesit me rreziqet që lidhen me përdorimin e burimeve ICT,
- të përcaktojë masat për mbrojtjen e informacionit nga zbulime të paautorizuara ose keqpërdorime.

Përdoruesit kontraktualë përdorin të gjitha burimet SIG ICT me kujdesin, efikasitetin dhe përgjegjësinë e duhur.

SIG mbron punonjësit dhe pronën e vet në masën maksimale të mundshme kundrejt aktiviteteve të paligjshme ose të dëmshme, të qëllimshme ose jo, nga individët.

Përdorimi i papërshtatshëm i IT vë SIG dhe përdoruesit e saj në rreziqe, si infektime virale të kompjuterit duke prekur sistemet e IT, kërcënime ndaj sistemeve dhe shërbimeve të rrjetit dhe keqpërdorim të informacionit dhe të të dhënave të ruajtura në sistemet e informacionit të SIG.

3 KËRKESA TË PËRGJITHSHME

- Ofruesi pajtohet me të gjitha ligjet dhe rregulloret e zbatueshme, duke përfshirë Rregulloren e Përgjithshme për Mbrojtjen e të Dhënave (GDPR) dhe Aktin e Rezistencës Operacionale Dixhitale për sektorin financiar (DORA).
- Ofruesi cakton një person kontakti për komunikimet e sigurisë dhe përgjigjet për incidentet.

4 MENAXHIMI I AKSESIT

- Ofruesi vendos kontrolle të rrepta për të parandaluar aksesin e paautorizuar në sistemet SIG ICT.
- Ofruesi siguron se në sistemet SIG ICT ka akses vetëm personeli i autorizuar, i verifikuar dhe trajnuar siç duhet.

- Menaxhimi i aksesit zbatohet për të gjitha format e aksesit në burimet ICT, duke përshirë, por pa kufizim:
  - aksesin e përdoruesit nëpërmjet ndërfaqeve grafike të përdoruesit (GUI),
  - aksesin nëpërmjet ndërfaqeve programuese të aplikacionit (API),
  - aksesin në sistem/shërbim (llogaritë e shërbimit),
  - aksesin administrativ dhe të privilegjuar,
  - skripte, Cron Jobs dhe integrime të automatizuara,
  - aksesin nga distanca (VPN, RDP, SSH etj.),
  - aksesin nëpërmjet pajisjeve celulare ose resë kompjuterike.
- Mbrojtja e aksesit në sistemet SIG ICT përfshin, por pa kufizim, autentikimin me shumë faktorë (MFA) dhe parimin e privilegjit më të vogël.
- I gjithë aksesi te sistemet ose të dhënat e SIG evidentohet dhe monitorohet për të siguruar gjurmët audite.
- Ofruesi ruan dhe shqyrton rregullisht një listë të përditësuar të personelit të autorizuar me të drejta aksesi në sistemet SIG ICT .

5 MBROJTJA E TË DHËNAVE

- Ofruesi siguron integritet, konfidencialitet dhe disponueshmëri të të dhënave.
- Të gjitha të dhënat janë të enkriptuara gjatë transmetimit duke përdorur protokollin kriptografik TLS 1.2 ose më të ri.
- Të gjitha të dhënat joaktive, përfshirë të dhënat e rezervuara, janë të enkriptuara duke përdorur AES-256 ose një standard ekuivalent.
- Ofruesi siguron që kompjuterët e përdorur për të kryer shërbimin e kontraktuar të kenë rregullisht përditësime të korrigjimeve të sigurisë, të kenë të instaluar vetëm softuer të autorizuar dhe të jenë të mbrojtur me softuer antivirusi të përditësuar rregullisht.
- Ofruesi minimizon përpunimin dhe ruajtjen e të dhënave, dhe vetëm përpunon dhe ruan të dhëna që janë rreptësisht të nevojshme për të përmbushur detyrimet kontraktuale.
- Ofruesi shmang ruajtjen e panevojshme të të dhënave dhe siguron që të dhënat të fshihen ose anonimizohen pasi ruajtja e tyre të mos jetë më e nevojshme.
- Me përfundimin e marrëdhënies kontraktuale, ofruesi fshin të dhënat ose i kthen ato plotësisht në SIG, në mënyrë të sigurt.

6 MENAXHIMI I INCIDENTEVE

- Ofruesi ka një politikë të menaxhimit të incidenteve në fuqi që mbulon zbulimin, raportimin dhe zgjidhjen e incidenteve të sigurisë.
- Incidentet e sigurisë nga ofruesi, të cilat prekin SIG, raportohen te SIG brenda 24 orëve.
- Ofruesi i mundëson SIG të marrë pjesë në zgjidhjen e incidenteve që prekin sistemet e saj ICT, duke përfshirë dhënien e aksesit te dokumentet përkatëse.

7 REZISTENCA DHE VAZHDIMËSIA

- Ofruesi ka një plan për vazhdimësinë e biznesit (BCP) dhe një plan për rikuperimin nga shkatërrimi (DRP), dhe të dy testohen vazhdimisht.
- Këto plane testohen çdo vit dhe rezultatet i ofrohen SIG, me kërkesë të kësaj të fundit.

8 MENAXHIMI I NËNKONTRAKTORËVE LIDHUR ME SHËRBIMIN E KONTRAKTUAR

- Ofruesi merr miratim me shkrim nga klienti (SIG) përpara përfshirjes së nënkontraktorëve ose palëve të treta.
- Ofruesi siguron që të gjithë nënkontraktorët të plotësojnë të njëjtat kërkesa që zbatohen për ofruesin.

9 AUDITI DHE VLERËSIMI I RREZIKUT

- Ofruesi kryen rregullisht vlerësime të rrezikut në lidhje me shërbimet e veta dhe përfshin klientin (SIG) siç është e përshtatshme.
- Klienti (SIG) do të kryejë vetë vlerësimin e rrezikut të ofruesit, i cili mund të përfshijë pyetësorë për sigurinë dhe kryerjen e vlerësimeve të pavarura për masat e sigurisë.
- Me kërkesë të klientit, ofruesi i mundëson SIG raportet e auditit dhe testit, përgjigjet e pyetësorëve për sigurinë dhe bashkëpunon në mënyrë të arsyeshme për vlerësimet e pavarura.
- Klienti (SIG) rezervon të drejtën për të kryer rregullisht audite dhe vlerësime të pavarura të masave të sigurisë së ofruesit.
- Me kërkesë të klientit, ofruesi i mundëson SIG evidencat e pajtueshmërisë, si certifikata, raporte ose rezultate të testeve të sigurisë.

10 TRAJNIMI DHE NDËRGJEGJËSIMI

- Ofruesi i trajnon rregullisht punonjësit e vet që punojnë për klientin (SIG) për praktikat më të mira të sigurisë së informacionit dhe përmbajtje të tjera, siç kërkohet nga SIG.

11 PËRFUNDIMI I BASHKËPUNIMIT

- Me përfundimin e kontratës, ofruesi garanton shkëputjen e sigurt të shërbimeve nga sistemet SIG ICT, duke përfshirë çaktivizimin e aksesit dhe fshirjen në mënyrë të sigurt të të gjitha të dhënave të SIG.
- Pas përfundimit të kontratës, ofruesi mundëson një deklaratë ose formë tjetër të vërtetimit të fshirjes së të dhënave.

12 PËRDITËSIMET DHE NDRYSHIMET

- SIG rezervon të drejtën për ta përditësuar këtë dokument në mënyrë që të reflektojë ndryshimet lidhur me rreziqet, teknologjitë ose rregulloret. Ofruesi do të njoftohet për përditësimet dhe do të sigurojë pajtueshmërinë brenda një afati kohor të arsyeshëm.

13 PËRKUFIZIME DHE AKRONIME

Nr.	Termi/akronimi	Përshkrimi
3	**SIG**	Sava Insurance Group
4	**ICT**	Teknologjia e Informacionit dhe Komunikimit - një teknologji që mundëson mbledhjen, përpunimin dhe shkëmbimin e të dhënave

5	**MFA**	Autentikimi me shumë faktorë - një mënyrë autentikimi me shumë nivele që rrit sigurinë e aksesit
7	**AES-256**	Standard i Avancuar i Enkriptimit (256 bit) - një algoritëm kriptografik enkriptimi që përdoret për të mbrojtur të dhënat joaktive
8	**TLS 1.2**	Siguria e Shtresës së Transportit 1.2 – një protokoll kriptografik për komunikim të sigurt nëpër rrjete