1. Namen in usmeritev politike

ELLAB d.o.o. je specializirano podjetje za daljinski nadzor procesov, avtomatizacijo, telemetrijo in vzdrževanje rešitev za infrastrukturne objekte. Zaradi narave storitev, dolgoročnega sodelovanja z naročniki ter vloge v dobaviteljski verigi organizacij, ki zagotavljajo bistvene oziroma pomembne storitve, je informacijska in kibernetska varnost ena od temeljnih zahtev poslovanja družbe.

S to politiko določamo krovne zaveze vodstva in zaposlenih za vzpostavitev, izvajanje, vzdrževanje in nenehno izboljševanje sistema upravljanja varovanja informacij (SUVI / ISMS), skladno z zahtevami in načeli standarda ISO/IEC 27001:2022, relevantnimi dobrimi praksami in zahtevami zakonodaje, zlasti ZInfV-1 oziroma zahtevami, ki izhajajo iz prenosa direktive NIS 2 v slovenski pravni red.

2. Področje uporabe

Politika velja za vse poslovne procese, informacijska sredstva, podatke, sisteme, aplikacije, omrežja, projekte, storitve, lokacije in zaposlene v družbi ELLAB d.o.o. Uporablja se tudi za zunanje sodelavce, izvajalce, dobavitelje, partnerje in druge osebe, ki imajo dostop do informacij, sistemov, projektne dokumentacije ali infrastrukture družbe oziroma naročnikov.

Posebna pozornost je namenjena informacijam in sistemom, ki so povezani z načrtovanjem, programiranjem, konfiguriranjem, montažo, oddaljenim dostopom, vzdrževanjem, podporo in dokumentacijo rešitev za vodooskrbo, ravnanje z odpadnimi vodami, energetiko, okoljske meritve in druge infrastrukturne sisteme.

3. Temeljna načela informacijske varnosti

Pri varovanju informacij in sistemov upoštevamo naslednja načela:

- zaupnost – informacije so dostopne samo pooblaščenim osebam in samo v obsegu, ki je potreben za delo;
- celovitost – podatki, programska oprema, konfiguracije, zapisi in dokumentacija so točni, popolni in zaščiteni pred nepooblaščenimi spremembami;
- razpoložljivost – ključne informacije, sistemi in storitve so dostopni takrat, ko jih poslovni procesi in naročniki potrebujejo;
- sledljivost in odgovornost – pomembne aktivnosti se izvajajo na način, ki omogoča ustrezno identifikacijo, evidentiranje, nadzor in dokazovanje;
- odpornost dobavne verige – varnostne zahteve se upoštevajo tudi pri izboru, upravljanju in nadzoru dobaviteljev, zunanjih storitev in tehnoloških partnerjev.

4. Zaveze vodstva in varnostni cilji

Vodstvo ELLAB d.o.o. se zavezuje, da bo zagotavljalo ustrezne organizacijske, kadrovske, tehnične in finančne pogoje za izvajanje SUVI. Informacijska varnost se obravnava kot sestavni del kakovosti storitev, projektnega vodenja, razvoja, izvedbe, vzdrževanja in podpore naročnikom.

Krovni cilji SUVI so: zmanjševanje informacijskih in kibernetskih tveganj na sprejemljivo raven; varovanje informacij in sistemov naročnikov; zagotavljanje varnega razvoja, konfiguriranja in vzdrževanja rešitev; pravočasno zaznavanje in obravnava incidentov; zagotavljanje skladnosti z zakonskimi, pogodbenimi in standardizacijskimi zahtevami; krepitev zaupanja naročnikov, zaposlenih in partnerjev.

5. Upravljanje tveganj in varnostni ukrepi

Sistematično prepoznavamo, ocenjujemo in obvladujemo tveganja za informacijsko varnost. Tveganja presojamo glede na poslovni pomen informacij in sistemov, vpliv na naročnike, vpliv na varnost in neprekinjenost storitev ter morebitni vpliv na bistvene, pomembne ali kritične infrastrukturne funkcije.

Na podlagi ocene tveganj določamo varnostne ukrepe, med drugim: upravljanje dostopov in gesel; uporaba večfaktorske avtentikacije, kjer je to smiselno in izvedljivo; upravljanje oddaljenih dostopov; segmentacija in zaščita omrežij; varno upravljanje konfiguracij in sprememb; zaščita pred škodljivo programsko opremo; varnostno kopiranje; beleženje in spremljanje ključnih aktivnosti; fizično varovanje opreme in dokumentacije; varno ravnanje z nosilci podatkov; nadzor dobaviteljev; ter usposabljanje zaposlenih.

6. Varnost pri projektih, razvoju in vzdrževanju

Varnostne zahteve se vključujejo v vse faze življenjskega cikla rešitev: od zasnove, projektiranja in priprave dokumentacije do programiranja, izdelave elektro-krmilnih omar, testiranja, montaže, zagona, vzdrževanja in podpore. Spremembe na sistemih naročnikov se izvajajo nadzorovano, sledljivo in ob upoštevanju dogovorjenih pooblastil.

Pri oddaljenem dostopu, servisnih posegih in upravljanju konfiguracij uporabljamo načela najmanjših potrebnih pravic, ločevanja nalog, evidentiranja aktivnosti ter varnega prenosa in hrambe podatkov. Kadar obdelujemo ali hranimo dokumentacijo, konfiguracije, dostopne podatke ali tehnične informacije naročnikov, z njimi ravnamo kot z zaupnimi informacijami.

7. Skladnost, incidenti in neprekinjenost poslovanja

Spremljamo in upoštevamo relevantne zakonske, regulativne, pogodbene in standardizacijske zahteve, vključno z zahtevami s področja informacijske varnosti, varstva osebnih podatkov, varovanja poslovnih skrivnosti, kritične infrastrukture in dobavne verige. Posebno pozornost namenjamo zahtevam naročnikov, ki so zavezanci po ZInfV-1 ali poslujejo v okoljih z zvišanimi zahtevami kibernetske odpornosti.

Varnostni incidenti, ranljivosti, odstopanja in sumi zlorab se morajo nemudoma sporočiti odgovorni osebi za SUVI oziroma vodstvu. Družba zagotavlja postopke za evidentiranje, obravnavo, omejitev posledic, odpravo vzrokov, obveščanje prizadetih strani in učenje iz incidentov. Za ključne procese in informacijska sredstva se načrtujejo ukrepi neprekinjenega poslovanja in obnove delovanja.

8. Odgovornosti, ozaveščanje in izboljševanje

Za izvajanje te politike je odgovorno vodstvo družbe, vsak zaposleni in pogodbeni partner pa je odgovoren za varno ravnanje z informacijami, opremo, dostopi in dokumentacijo, ki so mu zaupani. Kršitve pravil informacijske varnosti se obravnavajo skladno z internimi akti, pogodbami in veljavno zakonodajo.

Politiko uresničujemo s katalogom politik, navodili, postopki, ocenami tveganj, evidencami, notranjimi presojami, vodstvenimi pregledi, usposabljanji in korektivnimi ukrepi. SUVI redno preverjamo in izboljšujemo na podlagi rezultatov presoj, incidentov, sprememb v poslovnem in tehnološkem okolju, zahtev naročnikov, sprememb zakonodaje ter ciljev družbe.

V Ljubljani, 17. 8. 2026
Tomaž Remih, direktor

ELLAB SINCE 1972
Ellab d.o.o.
Tbilisijska ulica 85
SI-1000 Ljubljana