Politika informacijske varnosti v skupini Krka

1 Namen in področje uporabe

Politika informacijske varnosti (v nadaljevanju Politika) velja za obvladujočo družbo Krka, tovarno zdravil, d. d., Novo mesto in njene odvisne družbe, ki skupaj sestavljajo Skupino Krka (v nadaljevanju Krka).

Politika določa načela in zaveze glede informacijske varnosti, ne vključuje pa zaupnih podrobnosti poslovanja, tehničnih nastavitev, notranjih postopkov in sklicev na interne dokumente. Politika zajema informacijska sredstva, ki se uporabljajo pri poslovanju, ne glede na njihovo obliko, lokacijo ali tehnološko platformo.

Določa javno objavljena načela, v skladu s katerimi Krka obvladuje in varuje informacije pred nepooblaščenim dostopom, razkritjem, spreminjanjem, uničenjem, prekinitvami, zlorabo ali izgubo. Opisuje Krkin pristop k upravljanju informacijske varnosti ter zavez glede zaupnosti, celovitosti, razpoložljivosti in avtentičnosti informacij.

Politika velja za vse zaposlene v Krki. Uporablja se tudi za pogodbene izvajalce, dobavitelje, ponudnike storitev in vse, ki dostopajo do Krkinih informacijskih sredstev. Zanje Krka zahteva varovanje informacij z uporabo ustreznih varnostnih praks in odgovornim ravnanjem.

V Krki okvir informacijske varnosti usklajujemo z uveljavljenimi mednarodnimi standardi in veljavnimi predpisi. Kadar so nacionalne zahteve strožje, ravnamo v skladu z njimi.

Krka informacije in podatke prepoznava kot ključna poslovna sredstva. Varujemo jih z odgovornim upravljanjem, obvladovanjem tveganj, usposabljanjem in rednim ozaveščanjem zaposlenih, preventivnim delovanjem in nenehnimi izboljšavami.

2 Upravljanje in odgovornost

Zagotavljamo mehanizme celostnega upravljanja za nadzor informacijske varnosti ter za njeno vključevanje v poslovno načrtovanje, obvladovanje tveganj in operativno odločanje na nivoju Krke.

Informacijska varnost je skupna odgovornost vseh zaposlenih v Krki. Uprava Krke zagotavlja usmeritve upravljanja in nadzora informacijske varnosti. Pooblaščenec za informacijsko varnost usklajuje sistem upravljanja, sodeluje pri prepoznavanju in obvladovanju tveganj, spremlja učinkovitost vzpostavljenih sistemov in spodbuja nenehno izboljševanje na področju informacijske varnosti. Oseba, odgovorna za neprekinjeno poslovanje, nadzoruje sistem upravljanja neprekinjenega poslovanja, pooblaščenec za varstvo podatkov pa zagotavlja podporo pri varstvu osebnih podatkov. Varnostni inženiring v okviru informacijske tehnologije aktivno spremlja, preverja in ocenjuje varnost informacijskega okolja.

Lastniki informacij so odgovorni za varovanje in nadzor informacij, ki nastajajo v njihovih procesih, vključno z njihovo razvrstitvijo, prepoznavanjem povezanih groženj in tveganj, odobravanjem in pregledovanjem pravic dostopa, ločevanjem nezdružljivih nalog ter varnim ravnanjem z informacijami, njihovo hrambo in varnim odstranjevanjem v celotnem življenjskem ciklu. Kadrovski sektor in druge funkcije, ki obdelujejo osebne podatke zaposlenih in drugih oseb, zagotavljajo varnost osebnih podatkov skladno z veljavnimi predpisi.

Nadzor nad sistemom upravljanja informacijske varnosti izvajamo preko Krkinih korporativnih odborov. Ti odbori spremljajo izvedbo pregledov sistema upravljanja informacijske varnosti, pregledujejo in potrjujejo ocene tveganj ter načrte obravnave tveganj, preučujejo rezultate notranjih presoj in ocen skladnosti ter spremljajo učinkovitost izvedbe varnostnih ukrepov.

Pooblaščenec za informacijsko varnost najmanj enkrat letno poroča o učinkovitosti, ustreznosti in skladnosti upravljanja informacijske varnosti. Za sprejemanje ključnih odločitev v zvezi s tem sistemom je pristojna uprava Krke.

3 Načela in zaveze informacijske varnosti

Zaupnost

Informacije so dostopne le pooblaščenim osebam, z njimi pa se ravna glede na njihovo občutljivost in upravičene poslovne potrebe.

Celovitost in avtentičnost

Informacije so zaščitene pred nepooblaščenim ali nenamernim spreminjanjem. V Krki si prizadevamo zagotavljati točnost, popolnost, zanesljivost in preverjanje informacij.

Razpoložljivost in odpornost

Informacije in podporne storitve so na voljo, ko so potrebne. Preventivno delovanje z ukrepi za zagotavljanje odpornosti, neprekinjenega poslovanja ter obnovitev podatkov in sistemov podpirajo ključne poslovne dejavnosti.

Varovanje na podlagi ugotovljenih tveganj

Varnostne ukrepe izvajamo glede na ugotovljena tveganja, poslovne potrebe, predpise ter priznane dobre prakse.

Varovanje informacij v celotnem življenjskem ciklu

Informacije varujemo pri njihovem nastanku, uporabi, izmenjavi, shranjevanju, hrambi in varnem odstranjevanju.

Odgovorno načrtovanje in uvajanje sprememb

Zahteve informacijske varnosti upoštevamo pri načrtovanju ali uvajanju poslovnih procesov, tehnologij in storitev ter pri izvajanju pomembnih sprememb.

Upravljanje pravice dostopa

Pravice dostopa dodeljujemo glede na vlogo in poslovne potrebe ter jih redno preverjamo.

Nenehno izboljševanje

Kot odziv na spreminjajoče poslovno okolje tveganja pregledujemo in ocenjujemo ter izboljšujemo sistem upravljanja informacijske varnosti, prakse, ukrepe in zmogljivosti.

Razmejitev odgovornosti

Odgovornosti in pooblastila so jasno določena in razmejena, s ciljem preprečevanja nasprotja interesov.

Skladnost in sodelovanje

Izpolnjujemo veljavne predpise in pogodbene obveznosti, skladno z njimi prijavljamo morebitne incidente ter sodelujemo s pristojnimi organi.

4 Upravljanje informacijske varnosti

Vzdržujemo sistem upravljanja informacijske varnosti, ki je strukturiran okvir za določanje ciljev v zvezi z informacijsko varnostjo, obvladovanjem tveganj, izvajanjem ukrepov, ocenjevanjem uspešnosti in izboljševanjem informacijske varnosti. Spoštujemo naslednje zaveze:

4.1 Obvladovanje tveganj in ranljivosti

Prepoznavamo in ocenjujemo tveganja informacijske varnosti ter izvajamo ustrezne ukrepe za njihovo obravnavo. Za odkrivanje ranljivosti, ocenjevanje izpostavljenosti in določanje prednostnih korektivnih ukrepov izvajamo analize ranljivosti in varnostne preglede.

Ocene tveganj izvajamo periodično ter po večjih organizacijskih spremembah, spremembah lokacije ali večjih spremembah informacijskih sistemov in storitev. Ocenjujemo grožnje, verjetnost njihovega nastanka in njihove morebitne posledice. Na tej podlagi prednostno določimo organizacijske, fizične in tehnične ukrepe, preostalo tveganje pa zmanjšamo na sprejemljivo raven. Pri tem upoštevamo tudi ustrezne zunanje dejavnike, ki bi lahko vplivali na informacijske sisteme in objekte.

4.2 Poročanje o incidentih in njihova obravnava
Vzpostavljeni so kanali za poročanje, prek katerih se lahko prijavijo incidenti, ranljivosti, varnostne pomanjkljivosti ali sumljive dejavnosti, povezane z informacijsko varnostjo. Prijave obravnavajo pooblaščene oziroma odgovorne osebe. Nadaljnji ukrepi se določijo glede na naravo in morebitni vpliv dogodka.

Incidente na področju informacijske tehnologije se prijavi na sos@krka.biz ali na telefonsko številko +386 7 331 2114 ali pooblaščencu za skladnost poslovanja na compliance.officer@krka.biz oziroma na telefonsko številko +386 7 331 2600.

4.3 Neprekinjeno poslovanje
Načrti neprekinjenega poslovanja ter obnove podatkov in sistemov podpirajo razpoložljivost ključnih informacijskih sistemov in storitev ob prekinitvah, ki jih vzdržujemo, preizkušamo in izboljšujemo v skladu s poslovnimi potrebami in tveganji.

4.4 Varstvo podatkov in informacij
Izvajamo ukrepe za varovanje podatkov in informacij v njihovem celotnem življenjskem ciklu. Informacije razvrščamo in obravnavamo glede na njihovo vrednost, občutljivost, veljavne predpise in poslovne zahteve. Hrambo in odstranjevanje upravljamo v skladu z veljavnimi predpisi.

4.5 Obveščanje pristojnih zunanjih organov o pomembnih incidentih
O pomembnih incidentih informacijske varnosti smo dolžni obveščati pristojne organe v rokih in na način, kot to določajo veljavni predpisi. Pooblaščene službe obveščanje in vso nadaljnjo komunikacijo usklajujejo v sodelovanju z odgovornim članom uprave ter pooblaščencem za informacijsko varnost. Navedeno velja tudi v Krkinih enotah v tujini, kjer lokalne odgovorne osebe komunicirajo s pristojnimi lokalnimi organi v sodelovanju s pristojnimi službami v matični družbi Krka in pooblaščencem za informacijsko varnost v matični družbi Krka. Javno komuniciranje o incidentih poteka v skladu s pravili korporativnega komuniciranja v Krki in v skladu z navodili pristojnega organa.

4.6 Varnostni ukrepi in kibernetska higiena
Izvajamo organizacijske, fizične in tehnične varnostne ukrepe, ki so sorazmerni z ugotovljenimi tveganji in veljavnimi zahtevami. Brez razkrivanja konfiguracij ali drugih operativnih podrobnosti ti ukrepi vključujejo naslednje:

- kibernetsko higieno in pravočasno posodabljanje programske opreme, vključno z odpravljanjem znanih ranljivosti;
- segmentacijo omrežij in ločevanje kritičnih sistemov, upravljanje podatkovnega prometa in komunikacij;
- upravljanje identitet in dostopa, vključno z večfaktorsko avtentikacijo;
- zaščito pred zlonamerno programsko opremo ter spremljanje in hrambo dnevnikov dejavnosti;
- ustrezno kriptografsko zaščito občutljivih informacij;
- redundanco kritične infrastrukture, varno izdelavo varnostnih kopij in redno preizkušanje obnovitve podatkov in sistemov;
- varnostno testiranje, vključno z neodvisnimi varnostnimi pregledi in vdornimi (penetracijskimi) testi;
- varno načrtovanje in izvajanje sprememb sistemov, omrežij in programske opreme;
- fizično in tehnično varovanje prostorov in opreme;
- spremljamo grožnje in ranljivosti na področju informacijske varnosti;
- sprotna ocena in obravnava varnostnih dogodkov ter ustrezno ukrepanje / eskalacija.

Učinkovitost izvedenih ukrepov se ocenjuje in izboljšuje na podlagi pregledov, testiranj in pridobljenih izkušenj.

4.7 Celovitost podatkov v reguliranih procesih

Informacije, ki nastajajo pri raziskavah in razvoju, proizvodnji, zagotavljanju kakovosti in drugih reguliranih procesih, se uporabijo kot dokaz o izvedenih dejavnostih in podlaga za sprejemanje odločitev. Zato upoštevamo zahteve glede celovitosti, točnosti, popolnosti, avtentičnosti in sledljivosti tovrstnih informacij, vključno z zahtevami, ki veljajo za računalniško podprte sisteme, elektronske zapise in elektronske podpise. Te informacije hranimo, arhiviramo in odstranjujemo v skladu z veljavno zakonodajo.

5 Kultura informacijske varnosti

V Krki spodbujamo kulturo varnega vedenja ter odgovornega ravnanja z informacijami in pravočasnega opozarjanja na morebitna tveganja.

Zaposlene ozaveščamo in usposabljamo na področju informacijske varnosti, da lažje prepoznajo grožnje ter razumejo lastno odgovornost, varovanje informacij in ustrezno uporabljajo informacijske vire. Aktivnosti ozaveščanja se redno posodabljajo glede na aktualne grožnje, tehnologije in načine dela.

Zaposleni:

- varujejo informacije, informacijske vire, poslovne skrivnosti in druge zaupne podatke, ki so jim zaupani;
- upoštevajo veljavne zahteve glede informacijske varnosti;
- odgovorno uporabljajo pravice dostopa in sredstva podjetja;
- poročajo o spremembah na svojem področju dela, ki bi lahko vplivale na informacijsko varnost ali neprekinjeno poslovanje;
- se udeležijo zahtevanih izobraževanj za ozaveščanje in usposabljanje glede informacijske varnosti;
- nemudoma prijavijo incidente, ogroženost in sumljive dejavnosti;
- sodelujejo pri pooblaščenih pregledih, preiskavah in korektivnih ukrepih.

6 Informacijska varnost pri sodelovanju s pogodbenimi in drugimi partnerji

Pri izvajanju Krkinih procesov ali obdelovanju njenih informacij lahko sodelujejo tretje osebe (dobavitelji, ponudniki storitev in druge tretje osebe). Zanje zahteve glede informacijske varnosti določamo sorazmerno z vrsto storitve, obsegom dostopa in povezanimi tveganji.

Zahteve glede informacijske varnosti upoštevamo pri izbiri sodelovanja s pogodbenimi in drugimi partnerji, sklepanju pogodb, vključevanju, izvajanju storitev, spremembah in prenehanju sodelovanja.

Varnostne prakse teh partnerjev, ki so pomembne za Krko, ocenjujemo in spremljamo izpolnjevanje dogovorjenih zahtev. Partnerji Krko obveščajo o varnostnih incidentih ter sodelujejo pri obvladovanju tveganj, preiskavah, odpravljanju posledic in aktivnostih za zagotavljanje neprekinjenega poslovanja.

Zahteve glede informacijske varnosti uveljavljamo tudi v dobavni verigi informacijske in komunikacijske tehnologije (IKT). Dobavitelje storitev IT, ponudnike storitev v oblaku in druge partnerje, ki obdelujejo Krkine informacije ali pomembno vplivajo na Krkino informacijsko varnost ali neprekinjeno poslovanje, skrbno izberemo, ocenimo z vidika tveganj in na različne načine presojamo. Varnostne zahteve so vključene v pogodbe ter specifikacije storitev in izdelkov. Izpolnjevanje teh zahtev spremljamo, dokazila o opravljenih ocenah pa hranimo. Pripravimo tudi načrte za izstop, ki omogočajo prehod na druge rešitve ali prenehanje storitev brez pomembnega vpliva na Krkino poslovanje.

7 Preverjanje, certificiranje in izboljševanje

7.1 Notranje in zunanje preverjanje

Izvajamo notranje presoje in preglede infrastrukture, informacijske tehnologije ter sistema upravljanja informacijske varnosti. Ocene tveganj, analize ranljivosti, vodstveni pregledi in druge aktivnosti preverjanja pomagajo pri ocenah, ali so ukrepi še vedno ustrezni in učinkoviti.

Zagotavljamo neodvisne zunanje presoje in ocene Krkinega sistema upravljanja informacijske varnosti ter okolja informacijske tehnologije. Te aktivnosti so dodatno varnostno zagotovilo, omogočajo pa tudi prepoznavanje možnosti za izboljšanje upravljanja, obvladovanja tveganj in ukrepov.

7.2 Zavezanost standardu ISO/IEC 27001 in ocenjevanje skladnosti ter poročanje

Zavezani smo ohranjanju že pridobljenega certifikata ISO/IEC 27001 za sisteme upravljanja informacijske varnosti, ki vključuje neodvisno zunanjo presojo. Ohranjanje tega certifikata podpira sistematičen pristop k informacijski varnosti, ki omogoča obvladovanje tveganj in nenehno izboljševanje.

Redno pregledujemo in posodabljamo Izjavo o uporabnosti, v kateri je opredeljeno, kako obravnavamo ukrepe iz standarda ISO/IEC 27001. Skladnost z veljavnimi predpisi na področju informacijske varnosti redno in periodično ocenjujemo in rezultate dokumentiramo. Določamo korektivne in preventivne ukrepe in njihovo izvajanje spremljamo do njihovega zaključka.

8 Sodelovanje s pristojnimi organi na področju informacijske varnosti

Pristojnim organom posredujemo vsa obvestila in razkritja, ki jih zahtevajo veljavni predpisi ali pristojni organi.

Sodelujemo s pristojnimi nacionalnimi organi, nacionalnimi službami za odzivanje na kibernetske incidente, nadzornimi organi za varstvo osebnih podatkov, zunanjimi strokovnjaki, strokovnimi organizacijami in interesnimi skupinami.

Spremljamo veljavne predpise, priporočila, smernice in standarde ter vključujemo potrebne spremembe v Krkin sistem upravljanja informacijske varnosti. Prav tako spremljamo zunanje vire informacij o novih grožnjah ter jih upoštevamo pri ukrepih za preprečitev in odkrivanje teh groženj.

9 Končne določbe

Politiko je sprejela uprava Krke, tovarne zdravil, d. d., Novo mesto na 13. redni seji dne 21. 10. 2026.

Politika je javni dokument in je objavljena na Krkini spletni strani. Pregleda in po potrebi posodobi se najmanj enkrat na pet let ter ob pomembnih spremembah veljavnega pravnega okvira. Vse spremembe in dopolnitve mora odobriti uprava.