

NAKA

Politika zagotavljanja kakovosti in upravljanja informacijske varnosti

POL

DATUM

12. 07. 2024

VERZIJA

2.1

DRUŽBA

Eligma d.o.o. / Letališka cesta 33F / Ljubljana, Slovenia

Informacije o dokumentu

Ime dokumenta:	Politika zagotavljanja kakovosti in upravljanja informacijske varnosti
Oznaka dokumenta:	POL
Stopnja zaupnosti:	Javno
Status:	Končna različica
Verzija:	2.1
Datum sprejema:	12. 07. 2024
Avtorji:	Luka Planinc, Timotej Polach, David Miroslavljevič
Skrbnik:	David Miroslavljevič, Vodja zagotavljanja kakovosti
Sprejel:	David Miroslavljevič

Zgodovina dokumenta

Verzija	Datum sprejema:	Status:
1.0	03. 05. 2021	Končna različica
2.0	21. 06. 2021	Končna različica
2.1	12. 06. 2024	Končna različica – popravek točke celovitost in avtentičnost

Zaupnost podatkov in avtorske pravice

Vsebina tega dokumenta je zaščitena v skladu z dodeljeno oznako zaupnosti, ki je lahko 'zaupno', 'interno' ali 'javno'. Vsaka uporaba, razkritje ali razmnoževanje vsebine tega dokumenta brez ustreznega dovoljenja je strogo prepovedana in se smatra kot kršitev notranjih pravil družbe Eligma d.o.o. in veljavne zakonodaje o varovanju poslovnih skrivnosti.

Vse avtorske pravice tega dokumenta so last družbe Eligma d.o.o. Kakršnokoli nepooblaščen kopiranje, distribucija ali druga uporaba dokumenta ali njegove vsebine je prepovedana.

POLITIKA ZAGOTAVLJANJA KAKOVOSTI IN UPRAVLJANJA INFORMACIJSKE VARNOSTI

Glede na vizijo družbe ter glede na stopnjo zavedanja in odgovornosti za izvajanje sistema vodenja kakovosti in upravljanja informacijske varnosti (v nadaljevanju: **sistem vodenja**) je vodstvo družbe določilo politiko zagotavljanja kakovosti in upravljanja informacijske varnosti (v nadaljevanju: **Politika** ali **PZKUIV**), ki definira cilje zagotavljanja kakovosti izdelkov in storitev družbe ter cilje zagotavljanja informacijske varnosti.

Namen sistema vodenja je omogočiti kakovostno oceno kvalitete rezultatov, spremljanje skladnosti rezultatov z načrti, tehničnimi specifikacijami in dobro prakso, zagotavljati neprekinjeno informacijsko varnost, redno obveščati ključne osebe z rezultati in vsebinami ter jim s tem omogočiti pravočasno predložitev pripomb in stališč in s tem uvedbo korektivnih ukrepov ter izboljšav. Kakovost rezultatov je izrednega pomena za zadovoljevanje določenih in/ali pričakovanih potreb odjemalcev ter končnih uporabnikov naših produktov in storitev. Zagotavljanje kakovosti je enako pomembno za kakovost rezultatov, ki jih dosežejo izvajalci, kot tudi za tiste, ki jih dosežejo zaposleni.

Namen PZKUIV je postaviti osnovna varnostna izhodišča za zaščito informacijskih sredstev družbe pred nevarnostmi, bodisi notranjimi ali zunanjimi, namernimi ali naključnimi. Zato Politika vsebuje obvezujoča pravila, ki se nanašajo na splošna načela ravnanja, dostopa, obdelave, shranjevanja, prenosa in uničevanja informacijskih podatkov znotraj družbe. Je dokument, ki ga morajo upoštevati in mu slediti vsi, ki imajo dostop do informacijskih sredstev družbe – direktor, zaposleni, pa tudi tretje osebe.

Zagotavljanje kakovosti produktov in storitev se izvaja predvsem z izvajanjem ocene kakovosti, ki se izdelava za vse večje produkte in storitve. Zagotavljanje kakovosti procesov informacijske varnosti se izvaja z letnimi notranjimi presojami. Ključnega pomena za zagotavljanje PZKUIV je, da se pri ocenjevanju kakovosti poskuša zagotoviti najvišjo možno raven neodvisnosti. Oceno opravljajo neodvisni posamezniki, ki niso vključeni v postopek priprave rezultatov in ciljev posameznega procesa.

Vodstvo družbe zagotavlja PZKUIV tako, da:

- seznanja in opozarja zaposlene, kako pomembno je dosledno izpolnjevanje zahtev v povezavi s produkti in storitvami, kako pomembna je informacijska varnost ter kako pomembno je dosledno upoštevanje zakonodaje ter drugih pravnih zahtev;
- skrbi za izvajanje sistema vodenja, s katerimi so seznanjeni vsi zaposleni;
- redno pregleduje Poslovnik vodenja in z njim povezane dokumente;
- zagotavlja, da so cilji kakovosti na sistemskem, procesnem, projektnem in produktnem nivoju vedno jasno določeni;
- zagotavlja razpoložljivost virov;
- skrbi, da se procesi in postopki za zagotovitev kakovosti in informacijske varnosti dosledno izvajajo v vseh fazah življenjskega cikla produktov in storitev;
- spremlja in nadzoruje izvajanje razvojnih nalog ter pregleduje poročila o njihovem napredku;
- podpira izvajanje meritev in analiz poslovanja ter na podlagi njihovih rezultatov vsaj 1x letno ugotavlja, v kolikšni meri so doseženi cilji na področju kakovosti;
- izvaja vodstvene preglede;
- določa potrebne korektivne ukrepe;
- s programi izboljšav postavlja nove, višje cilje.

Postopki zagotavljanja kakovosti so v grobem razdeljeni na postopke, ki vključujejo načrtovanje kakovosti, tj. opredelitev standardov kakovosti (ko jih je mogoče opredeliti) in opredelitev potrebnih dejavnosti za oceno kakovosti, ter postopke, ki se dejansko uporabljajo za ocenjevanje kakovosti rezultatov. Rast kakovosti v družbi odločilno temelji na dolgoročnem planu izboljšanja kakovosti. Le-to dosežemo prek naslednjih korakov:

1. **Načrtovanje:** Določitev temeljnih standardov, ki jim mora družba nenehno slediti za zagotavljanje visoke ravni kakovosti in informacijske varnosti. Zahteva postavitev konkretnih strateških ciljev zagotavljanja kakovosti ter informacijske varnosti v družbi, ki natančno določajo usmeritev, ki ji mora družba slediti, da zadosti ravni kakovosti in informacijske varnosti, ki si jo je zadala. Poleg določitve temeljnih standardov proces načrtovanja zahteva tudi določitev ukrepov za obravnavanje tveganj in priložnosti.
2. **Delovanje in izvedba:** Določitev zahtev za izdelke in storitve, določitev zahtev za preverjanje dobaviteljev; določitev in obvladovanje procesov za razvoj izdelkov in storitev.
3. **Vrednotenje izvedbe:** Notranja presoja in vodstveni pregled.
4. **Ukrepanje:** Glede na ugotovljene rezultate delovanja sistema vodenja vodstvo sprejme ustrezne odločitve o korektivnih in preventivnih ukrepih, s katerimi se odstranijo in preprečijo vzroki in neskladja.

Navedeni elementi procesa sistema vodenja zagotavljajo izpolnitev zahtev za kakovost izdelkov in storitev ter zahtev v pogledu upravljanja informacijske varnosti, kot varovanje:

- **zaupnosti in tajnosti:** varovanje poslovnih in osebnih podatkov ter drugih pomembnih informacij pred razkritjem nepooblaščenim osebam in zagotavljanje odgovornosti za opravljene storitve;
- **celovitosti:** Obravnava zagotavljanje pravilnosti ter celovitosti informacij in programske opreme. Kontrola celovitosti se uporablja za zaščito podatkov in sistemov pred nepooblaščenimi spremembami. Celovitost olajša ugotavljanje sprememb ter preprečuje, da bi spremenjeno kopijo obravnavali kot original.
- **avtentičnosti:** Avtentičnost se nanaša na pristnost in nepotvorjenost podatkov, informacij in sistemov, v stanju, obliki in kvaliteti kakršni so.
- **razpoložljivosti in dostopnosti:** varovanje podatkov, informacij in storitev pred prekinitvami v delovanju ter zagotavljanje informacij pooblaščenim uporabnikom v ustreznem času in na ustrezen način.