



Panteon Group® D.O.O.  
Cesta Jaka Platiše 13  
4000 Kranj

# **Krovnna politika varovanja informacij v podjetju Panteon Group®**

*Verzija 3*

*Kranj, 25.03.2009*

*Dokument je vzdrževan v informacijskem sistemu za upravljanje dokumentov sistema vodenja organizacije Panteon Group®  
d. o. o., kjer je dosegljiva trenutno veljavna verzija.  
Uporabnik je odgovoren, da preveri skladnost tega izvoda z zadnjo veljavno izdajo.*

## KROVNA POLITIKA VAROVANJA INFORMACIJ V PODJETJU Panteon Group® D.O.O.

### 1. NAMEN

Podjetje Panteon Group® d.o.o. se zaveda vrednosti informacij in informacijskega sistema. Za uspešno poslovanje podjetja so varne in zanesljive informacije in informacijska sredstva ključnega pomena. V ta namen podjetje vodi sistem varovanja informacij, ki s svojimi politikami, pripadajočimi organizacijskimi predpisi in delovnimi navodili določa, kako informacijsko premoženje zaščititi. S krovno politiko varovanja informacij vodstvo izraža svojo odgovornost in zavezanost k zagotavljanju ustrezne varnosti informacijskega premoženja, zaposleni, pogodbeni delavci in vsi uporabniki informacij in informacijskega sistema pa svojo odgovornost glede izvajanja varnostne politike podjetja Panteon Group®.

Cilj varovanja informacij je preprečevati oziroma zmanjšati posledice varnostnih incidentov na najmanjšo možno mero ter zagotavljati neprekinjeno poslovanje. Namen varnostne politike je ugotoviti pomembnost informacij za poslovanje podjetja in jih ustrezno zaščititi v smislu zagotavljanja zaupnosti, celovitosti in razpoložljivosti.

- **zaupnost:** zagotoviti dostop do informacij samo pooblaščenim osebam
- **celovitost:** varovanje točnosti in popolnosti informacij s preprečevanjem nepooblaščenih sprememb
- **razpoložljivost:** zagotavljanje pooblaščenim osebam dostop do informacij in z njimi povezanimi sredstvi, ko jih potrebujejo

Politika varovanja informacij določa varnostne ukrepe in postopke v skladu z varnostno občutljivostjo, poslovno vrednostjo in kritičnostjo informacij ne glede na obliko, v kateri se informacije pojavljajo: na računalnikih, na papirju ali na prenosnih pomnilniških medijih ter pri prenosu preko omrežja oziroma pri ustnem posredovanju.

Zaradi vse večje odvisnosti poslovanja od informacijske tehnologije se povečuje ranljivost za različne zunanje in notranje grožnje, ki postajajo čedalje bolj razširjene, prefinjene in učinkovite pri povzročanju poslovne škode podjetju. Varnostna politika v obliki varnostnih kontrol postavi celovit okvir za zagotavljanje varnosti informacij in informacijskega sistema pred grožnjami kot so napake, motnje, poneverbe, sabotaze, kršenje zaupnosti, prekinitve delovanja, kraje in naravne nesreče.

### 2. Obseg varnostne politike

Varnostne politike, navodila in postopki varovanja informacij na nižjem nivoju pokrivajo vse poslovne procese za zagotavljanje informacijskih storitev podjetja Panteon Group®.

Politika varovanja informacij in informacijskih sistemov v podjetju Panteon Group® zajema vseh 11 področij določenih v standardu ISO/IEC 27002:2005, ki vsebujejo 133 varnostnih kontrol:

- 1. Politika varovanja**  
dokument o politiki varovanja informacij, pregledovanje politike varovanja informacij
- 2. Organiziranost varovanja**  
obvladovanje varovanja informacij v organizaciji in dostopa tretjih strank do naprav informacijske tehnologije
- 3. Upravljanje s sredstvi**  
opredelitev lastnikov informacijskih sredstev, odgovornosti za varnostne ukrepe, varnostna razvrstitev informacij
- 4. Varovanje v zvezi z osebjem**  
ustrezno preverjanje kandidatov za zaposlitev, izjava o zaupnosti, usposabljanje uporabnikov za varnostne postopke in pravilno uporabo naprav informacijske tehnologije, upravljanje s prenehanjem delovnih razmerij in spremembami odgovornosti
- 5. Fizično in okoljsko varovanje**  
fizična zaščita varovanih območij pred nepooblaščenim dostopom, škodo in motnjami, fizična zaščita informacijske opreme, električne napeljave in kabelskega omrežja pred ogrožanjem varnosti in nevarnostmi iz okolja
- 6. Upravljanje s komunikacijami in obratovanjem**  
vzpostavitev odgovornosti in postopkov za obratovanje vseh računalnikov in omrežij ter ravnanje z njimi, načrtovanje in priprava za zagotovitev primernih zmogljivosti sistema, zaščita pred zlonamerno programsko opremo, politika izdelave rezervnih kopij podatkov, varovanje v računalniških omrežjih, ravnanje z nosilci podatkov in varovanje, obvladovanje izmenjave podatkov in programske opreme med organizacijami, nadzor informacijskih sistemov in beleženje varnostnih dogodkov
- 7. Obvladovanje dostopa do sistema**  
politika dostopa do sistemov, kontrola dodeljevanja pravice dostopa do informacijskih sistemov in storitev, odgovornosti uporabnikov, kontrola dostopa do operacijskega sistema, kontrola dostopa do aplikacij in informacij, obvladovanje uporabe prenosne računalniške opreme in dela na daljavo
- 8. Nabava, razvoj in vzdrževanje sistema**  
opredelitev varnostnih zahtev informacijskih sistemov, varnostne kontrole v aplikacijah, politika uporabe šifriranja podatkov, ravnanje z dostopom do sistemskih datotek in izvornih programov, varovanje razvojnega in vzdrževalnega okolja, upravljanje z ranljivostmi
- 9. Upravljanje z varnostnimi incidenti**  
postopki poročanja o varnostnih incidentih, odgovornosti in postopki ravnanja z varnostnimi incidenti
- 10. Upravljanje neprekinjenega poslovanje**  
razvoj in vzdrževanje ustreznih načrtov za hitro ponovno vzpostavljanje pomembnih poslovnih procesov in storitev v primeru resnih prekinitev poslovanja
- 11. Usklajenost**  
usklajenost z zakonskimi zahtevami, usklajenost z varnostno politiko in tehnična usklajenost, upoštevanje revidiranja sistemov

### **3. Splošna odgovornost in odgovornost za posamezna področja varovanja informacij**

Vodstvo podjetja je odgovorno za vpeljavo sistema vodenja varovanja informacij, za spremljanje in nadziranje učinkovitosti varnostnih ukrepov in postopkov.

Za upoštevanje in izvajanje posameznih varnostnih ukrepov in postopkov so zadolženi vsi zaposleni, vodstvo podjetja pa je odgovorno za izvajanje varnostne politike v celoti in za zagotovitev potrebnih finančnih in človeških virov.

Vodstvo podjetja določi odgovorno osebo za vzpostavitev, izvajanje in vzdrževanje procesov, ki so potrebni za sistem vodenja varovanja informacij po standardu ISO/IEC 27001:2005. Naloge odgovornega za varovanje informacij so :

- nadziranje spreminjanja dokumentov varnostne politike pri spremembah kot so varnostni incidenti, nove ranljivosti, spremembe v organizacijski in tehnični infrastrukturi
- najmanj enkrat letno ovrednotiti varnostna tveganja, ki grozijo podjetju
- na osnovi ocenjenih varnostnih tveganj, rezultatov presoj, pregledov in testiranj pripraviti načrt ukrepov za izboljšanje stanja informacijske varnosti
- priprava letnega plana in programa notranjih presoj
- zagotavljanje neodvisne presoje elementov sistema vodenja varovanja informacij
- stalno izboljševanje sistema vodenja varovanja informacij
- spremljanje in vrednotenje učinkovitosti sistema vodenja varovanja informacij ter poročanje vodstvu o njegovem delovanju in potrebah za izboljševanje
- zagotavljanje ozaveščenosti zaposlenih glede varovanja informacij ter ustrezne usposobljenosti, da razumejo varnostno politiko in varnostne ukrepe
- komuniciranje z zunanjimi strankami v zadevah, ki se nanašajo na sistem vodenja varovanja informacij.

#### **4. Odgovornosti zaposlenih pri poročanju varnostnih kršitev in varnostnih pomanjkljivosti**

V proces stalnega izboljševanja varnosti informacij in informacijskih sredstev morajo biti vključeni vsi zaposleni. Naloga odgovornega za varovanje informacij je, da zaposlene ustrezno seznanji z varnostnimi zahtevami in kontrolami ter jih usposobi za varno uporabo informacij, informacijskih sredstev in naprav informacijske tehnologije .

Zaposleni morajo sporočiti opažene varnostne incidente kot so:

- opažene varnostne pomanjkljivosti
- namerne in nenamerne varnostne kršitve
- nepravilno ali sumljivo delovanje sistemov ali programske opreme
- nedelovanje sistemov
- viruse
- napake
- grožnje in ranljivosti sistemov in storitev
- vse nenačrtovane aktivnosti na sistemih, ki niso del rednega vzdrževanja

osebi odgovorni za varovanje informacij. Varnostne incidente morajo zaposleni prijavijo čim prej ustno, telefonsko na številko 040 522 677 ali po elektronski pošti na naslov [varnost@panteongroup.com](mailto:varnost@panteongroup.com), ter tako odgovornemu za varovanje informacij omogočiti čimprejšnje ustrezno ukrepanje.

Odgovorni za varovanje informacij prijave varnostnih incidentov zbira, pregleduje in analizira, po potrebi takoj obvesti vodstvo, nanje pravočasno reagira z ustreznimi ukrepi oziroma koordinira izvajanje potrebnih aktivnosti. O kritičnih varnostnih incidentih odgovorni za varovanje informacij poroča na rednih sestankih varnostnega foruma. Varnostni forum na podlagi poročila odloča o potrebnih ukrepih, s katerimi bi preprečili ponavljanje varnostnih incidentov. V primeru suma kršenja zakona mora zaposleni, ki je zaznal incident, o tem obvestiti direktorja, ki je odgovoren za vsa nadaljnja postopanja, vključno za obveščanje ustreznih uradnih organov.

Uporabniki računalniških storitev pod nobenim pogojem ne smejo dokazovati sumov o pomanjkljivosti varovanja informacij in ranljivosti sistemov.

## 5. Pojasnilo posebnih varnostnih ukrepov

Ukrepi varnostne politike informacijskega sistema so zaposlenim v celoti na voljo v elektronski obliki. Varnostne določbe v nadaljevanju pa predstavljajo ključne gradnike pri zagotavljanju varnosti.

- Politika čiste mize in čistega zaslona
- Ravnanje z gesli
- Politika obvladovanja dostopa do sistema
- Politika obvladovanja programske opreme
- Upravljanje mobilne računalniške opreme
- Uporaba Interneta in elektronske pošte na sistemih podjetja

## 6. Vzdrževanje varnostne politike

Ob spremembah zakonodaje, pojavu novih groženj, novih varnostni incidentov, spremembah organizacijske ali tehnične infrastrukture, ki vplivajo na varovanje informacij in informacijskih sistemov, se bo sistem varovanja informacij nenehno prilagajal z uvajanjem novih in dopolnjevanjem že obstoječih varnostnih ukrepov in postopkov. Dinamično prilagajanje varnostne politike v skladu s poslovnimi zahtevami in spremembami, ki vplivajo na prvotno oceno varnostnega tveganja, je zadolžitev odgovornega za varovanje informacij.

## 7. Upravljanje z dokumenti politike varovanja informacij

Dokumenti politike varovanja informacij so objavljeni v elektronski obliki, tako, da so na vpogled vsem zaposlenim in tretjim osebam, ki imajo dostop do informacij in informacijskega sistema podjetja. Vsak dokument politike varovanja informacij mora imeti skrbnika, ki je zadolžen za njegovo pravočasno obnavljanje in spreminjanje, ter osebo, ki dokument odobri. Imeni obeh sta zapisani v spodnjem levu kotu dokumenta. V vsakem dokumentu je označen tudi dan, ko je dokument stopil v veljavo.

Dopolnitev ali izboljšavo dokumenta lahko predlaga vsak zaposleni tako, da predlog naslovi na skrbnika ali varnostni forum. Ko so dokumenti spremenjeni in odobreni, jih je potrebno takoj objaviti in o spremembi obvestiti zaposlene in tiste tretje stranke, ki jih morajo upoštevati pri svojem delu..

## **8. Sankcije**

Vsako neupoštevanje pravil politike varovanja informacij in pripadajočih dokumentov se šteje za kršitev pogodbe o delu in se kot tako tudi sankcionira.