Panteon Group® D.O.O.
Vojkovo nabrežje 30A
6000 Koper - Capodistria

# Krovna politika varovanja informacij v podjetju Panteon Group®

***Verzija 5***

***Koper, 01.08.2024***

# 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 gleda 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, sabotaže, kršenje zaupnosti, prekinitev 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 vsa 4 področja določenih v standardu ISO/IEC 27001:2022, ki vsebujejo 93 varnostnih kontrol.

1. **Organizacijski nadzor**
2. **Nadzor nad ljudmi**
3. **Fizični nadzor**
4. **Tehnološki nadzor**

## 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 27001:2022. Naloge varnostnega inženirja 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 vzdrževanje sistema vodenja varovanja informacij
- spremljanje in obveščanje o varnostnih grožnjah

Ukrepe in naloge, ki jih podjetje prepozna kot permanentne za zagotavljanje potrebne varnosti informacij, podjetje opredeli v letnem planu aktivnosti , ki jih redno izvaja.

## 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 varnostnega inženirja je, da zaposlene ustrezno seznani 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

varnostnemu inženirju. Varnostne incidente morajo zaposleni prijavijo čim prej ustno, telefonsko na številko +386 40 435 058 ali po elektronski pošti na naslov varnost@panteongroup.com, ter tako varnostnemu inženirju omogočiti čimprejšnje ustrezno ukrepanje.

Varnostni inženir 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 varnostni inženir 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 pomanjkljivostih 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 (Upravljanje z informacijskimi sredstvi)
- Ravnanje z gesli (Nadzor dostopa do informacijskih sredstev)
- Politika obvladovanja dostopa do sistema (IT viri in omrežje)
- Politika obvladovanja programske opreme (Upravljanje z informacijskimi sredstvi)
- Upravljanje mobilne računalniške opreme (Politika mobilnih naprav)
- Uporaba Interneta in elektronske pošte na sistemih podjetja (Upravljanje z informacijskimi sredstvi)
- Uporaba kriptografskih ključev (Upravljanje z informacijskimi sredstvi)

## 6. Vzdrževanje varnostne politike

Ob spremembah zakonodaje, pojavu novih groženj, novih varnostnih 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 varnostnega inženirja.

## 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.