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

Okvirna politika zaštite informacija u kompaniji Panteon Group®

Verzija 4

Kopar, 15.03.2022.

OKVIRNA POLITKA ZAŠTITE INFORMACIJA U KOMPANIJI Panteon Group® D.O.O.

1. CILJ

Panteon Group® d.o.o. je u potpunosti svestan vrednosti informacija i informacionog sistema. Za uspešno poslovanje preduzeća od najvećeg značaja su informacije koje su pouzdane i koje se odnose na imovinu. Iz tog razloga, kompanija upravlja sistemom zaštite informacija koji uz pomoć, važećih politika, propisa koji se odnose na organizaciju i uputstava za rad, definiše kako na odgovarajući način zaštititi sredstva koja se odnose na informacije. Pomoću Okvirne politke zaštite informacija menadžment stavlja naglasak na svoju odgovornost i obavezu zaštite sredstava vezanih za informacije, pri čemu zaposleni, radnici po ugovoru, i svi korisnici informacija i sistema vezanih za informacije naglašavaju svoju odgovornost kada je reč o sprovođenju politike zaštite informacija Panteon Group®.

Cilj politike zaštite informacija je da se spreče ili ublaže posledice slučajeva vezanih za bezbednost, kao i da se obezbedi neometano poslovanje. Cilj ove politike zaštite informacija je da se odredi značaj informacija za poslovanje kompanije i da se zaštite na pravilan način, u smislu da se obezbedi njihova poverljivost, celovitost i dostupnost.

- **Poverljivost:** da se obezbedi dostupnost informacija isključivo ovlašćenim licima
- **Celovitost:** zaštita tačnosti i kompletnosti informacija sprečavanjem njihovog neovlašćenog menjanja.
- **Dostupnost:** obezbeđenje pristupa informacijama i sredstvima u vezi sa informacijama samo za ovlašćena lica kojima su iste neophodne i koja su u vezi sa sredstvima vezanim za informacije.

Politika zaštite informacija definiše mere zaštite a prema osetljivosti u odnosu na bezbednost, sa poslovnom vrednošću i kritičnošću informacija, bez obzira na formu u kojoj se informacije javljaju: u kompjuterima, na papiru ili u pokretnim medijima ili pri prenošenju kroz mrežu ili pri usmenom prenošenju.

Zbog sve naglašenije zavisnosti poslovanja od informacione tehnologije, ugroženost spoljašnjim i unutrašnjim opasnostima je sve veća, rafiniranija i uspešnija u nanošenju štete preduzeću. Politika koja se odnosi na bezbednost, u formi kontrole bezbednosti, uspostavlja integralni okvir za bezbednost informacija i zaštitu informacionog sistema od opasnosti, na primer grešaka, otkaza, poremećaja, falsifikovanja, sabotaže, kršenja obaveze tajnosti, prekida u radu, krađa i prirodnih katastrofa.

2. Nivo politike zaštite informacija

Politike, uputstva i procedure koje se odnose na niži nivo obuhvataju sve poslovne procese za obezbeđenje informacionih usluga koje pruža Panteon Group®.

Politika koja se odnosi na zaštitu informacija i informacionog sistema koju sprovodi Panteon Group® obuhvata svih 14 (četrnaest) područja, koja su definisana u Standardu ISO/IEC 27001:2013, sa 114 kontrole bezbednosti, tj:

1. **Politika zaštite informacije**
   zaštite koji se tiče politike zaštite informacija, preispitivanja i verifikacije politike zaštite
2. **Organizacija zaštite informacija**
   Upravljanje zaštitom informacija u okviru organizacije i upravljanje pristupom trećih lica sredstvima koja se odnose na informacionu tehnologiju.
3. **Zaštita u vezi sa zaposlenima**
   Odgovarajuća verifikacija kandidata za zapošljavanje, Izjava o poverljivosti, obuka/obrazovanje korisnika u vezi sa bezbednosnim procedurama i pravilnom upotrebom opreme u informacionoj tehnologiji, upravljanje prestankom radnog odnosa i upravljanje promenama u vezi sa odgovornostima kao i edukacija o bezbednosti informacija.
4. **Upravljanje informacijama kao sredstvima**
   Identifikacija vlasnika informacionih sistema, odgovornosti u vezi sa merama koje se odnose na zaštitu, klasifikacija informacija vezanih za bezbednost.
5. **Kontrola pristupa izvorima informacija**
   Definisanje vlasništva nad pravima i ograničenja pristupa informacijama izvora, mrežnih i IT izvora. Obezbediti ukidanje prava pristupa, korišćenje korisničkih imena i pravila za promenu i odabir lozinki, ograničiti pristup serverima i koristiti posebne kontrole za pristup izvornom kodu.
6. **Upotreba kriptografije**
   Upotreba kriptografije za prenos podataka i upotreba sertifikata za pristup dokumentima i aplikacijama.
7. **Fizička i zaštita životne sredine**
   Fizička zaštita obezbeđenih područja od neovlašćenog pristupa, fizička zaštita informacione tehnologije, zaštita elektro instalacija i kablovske mreže od bezbednosnih rizika i opasnosti koje potiču iz životne sredine.
8. **Sigurnost rada**
   Uspostavljanje odgovornosti i procedura rada i upravljanje svim računarima i mrežama, planiranje i priprema za obezbeđenje odgovarajućih sposobnosti sistema, zaštita od štetnih softvera, politika izrade rezervnih kopija podataka, zaštita u okviru računarskih mreža, upravljanje zaštitom medijuma za podatke, upravljanje razmenom podataka i računarskih programa između organizacija, kontrola informacionih sistema i evidentiranje slučajeva koji se odnose na bezbednost.
9. **Bezbednost komunikacija**
   Politika pristupa sistemima, kontrola dodele prava pristupa informacijskim sistemima i uslugama, odgovornosti korisnika, kontrola pristupa operativnom sistemu, kontrola pristupa aplikacijama i informacijama, upravljanje korišćenjem prenosne računarske opreme i daljinskog upravljača rad, interkonekcionu politiku, politiku razmene podataka sa dobavljačima i kupcima.
10. **Nabavka, razvoj i održavanje sistema**

Identifikacija zahteva koji se odnose na bezbednost informacionih sistema, kontrola bezbednosti u okviru aplikacija, upravljanje šifriranjem podataka, upravljanje pristupom sistemskim datotekama i izvornim programima, zaštita sredine koja se odnosi na razvoj i održavanje, upravljanje osetljivim mestima.

11. **Odnos sa partnerima i kupcima.**
    Potpisivanje ugovora o sigurnosti informacija sa klijentima i partnerima, evidentiranje pristupa informacijskim resursima.
12. **Upravljanje incidentima vezanim za bezbednost**
    Procedure koje se odnose na izveštavanje o incidentima vezanim za bezbednost, upravljanje odgovornostima za incidente vezane za bezbednost i procedurama .
13. **Upravljanje neometanim poslovanjem**
    Donošenje i održavanje odgovarajućih planova za brzi oporavak vitalnih poslovnih procesa u slučaju većeg prekida poslovnih aktivnosti.
14. **Usaglašenost**
    Usaglašenost sa zakonskim uslovima, usaglašenost sa bezbednosnim politikama i tehnička usaglašenost, razmatranje kontrole sistema.

3. Opšta odgovornost i odgovornost za pojedinačne oblasti zaštite informacija

Rukovodstvo kompanije je odgovorno za upravljanje sistemom zaštite informacija, za praćenje i nadgledanje efikasnosti u vezi sa merama i procedurama zaštite.
Za sprovođenje pojedinačnih mera i procedura bezbednosti odgovorni su svi zaposleni, a samo rukovodstvo kompanije je odgovorno za sprovođenje politike zaštite informacija u celini, kao i za obezbeđivanje potrebnih finansijskih i ljudskih resursa.

Rukovodstvo kompanije određuje i imenuje odgovorno lice za uspostavljanje, sprovođenje i održavanje procesa koji su potrebni za upravljanje sistemom zaštite informacija u skladu sa Standardom ISO/IEC 27001:2013. Zadaci menadžera sigurnosti su sledeći:

- nadgledanje dokumenata koja se tiču politike zaštite prilikom promena, na primer incidenti vezani za bezbednost, nova ugrožavanja, promene organizacione i tehničke infrastrukture;
- najmanje jednom godišnje procena bezbednosnih rizika koji ugrožavaju kompaniju;
- izrada planova unapređenja stanja bezbednosti informacija, na osnovu procenjenih bezbednosnih rizika, rezultata evaluacije, preispitivanja i testiranja;
- izrada godišnjih planova i programa ocenjivanja unutrašnje bezbednosti;
- obezbeđenje nezavisnog vrednovanja elemenata upravljanja sistemom zaštite informacija;
- stalno poboljšavanje upravljanja sistemom zaštite informacija;
- praćenje i vrednovanje efikasnosti upravljanja sistemom zaštite informacija i podnošenje izveštaja rukovodstvu o njegovom učinku i zahtevima za poboljšanje procesa;
- osiguranje svesti zaposlenih o upravljanja sistemom zaštite informacija i potrebnih kvalifikacija, sa ciljem da zaposleni razumeju politiku i mere zaštite informacija;

- komunikacije sa eksternim korisnicima koje se odnose na održavanja sistema upravljanja bezbednosti informacija.

Mere i zadatke, koje kompanija prepoznaje kao trajne u cilju obezbeđenje neophodne informacione bezbednosti, kompanija definiše godišnjim planom aktivnosti, koji redovno sprovodi.

4. Odgovornost zaposlenih za prijavljivanje incidenata vezanih za bezbednost i nedostataka vezanih za bezbednost

Svi zaposleni treba da budu uključeni u postupak poboljšanja informisanja i bezbednosti informacija kao sredstva. Zadatak menadžera sigurnosti je da se svi zaposleni pravilno upoznaju sa zahtevima i kontrolama koje se odnose na bezbednost i da se osposobe da informacionu tehnologiju koriste na bezbedan način.

Zaposleni moraju da prijave uočene incidente vezane za bezbednost, kao na primer:

- uočene nedostatke u vezi bezbednosti
- namerne i nenamerne povrede bezbednosti
- nepravilan i sumnjiv rad sistema i softvera
- loše funkcionisanje sistema
- viruse
- greške i otkaze
- opasnosti i ugrožavanje sistema i servisa
- sve neplanirane aktivnosti na sistemima koje nisu deo redovnog održavanja,

odgovornim licima za zaštitu informacija. Prijave incidenata vezane za bezbednosti neophodno je izvršiti što je pre moguće, usmeno pozivom na telefon (+386 40 435 058) ili e-poštom na adresu varnost@panteongroup.com, da bi menadžer sigurnosti bio u mogućnosti da reaguje bez odlaganja.

Menadžer sigurnosti prikuplja, pregleda, ocenjuje i analizira izveštaje koji se odnose na bezbednost , bez odlaganja obaveštava rukovodstvo, reaguje blagovremeno sprovođenjem odgovarajućih mera i koordinira potrebne aktivnosti. Menadžer sigurnosti podnosi izveštaje na redovnim sastancima foruma za bezbednost na osnovu kojih ovaj forum odlučuje o potrebnim merama, da bi se sprečilo ponavljanje incidenata vezanih za bezbednost. U slučaju sumnje u kršenja zakona, zaposleni koji je predvideo incident dužan je da obavesti rukovodioca, odgovornog za sve dalje procedure, uključujući izveštavanje nadležnih organa vlasti.

Korisnicima kompjuterskih servisa ni u kom slučaju nije dozvoljeno da dokumentuju svoje sumnje u pogledu nedostataka zaštite informacija i na ugroženosti sistema.

5. Objašnjenje specijalnih bezbednosnih mera

Politike zaštite informacionih sistema su dostupne zaposlenima u celosti u elektronskoj formi. Odredbe koje se odnose na bezbednost u nastavku ovog dokumenta predstavljaju glavne elemente za osiguranje bezbednosti:

- Princip čistog stola i čistog ekrana (Upravljanje sa informacionim sredstvima)
- Upravljanje lozinkama (Nadzor pristupa do informacionih sredstava)

- Politika pristupa upravljanju sistemom (IT resursi i mreže)
- Politika upravljanja softverom (Upravljanje sa informacionim sredstvima)
- Upravljanje mobilnom računarskom opremom (Politika mobilnih naprava)
- Upotreba Interneta i elektronske pošte na sistemima kompanije (Upravljanje sa informacionim sredstvima)
- Upotreba kripografskih ključeva (Upravljanje sa informacionim sredstvima)

6. Održavanje bezbednosne politike

Pri promeni zakona, pojavi novih opasnosti, novih incidenata vezanih za bezbednost, izmena organizacione i tehničke infrastrukture, koje mogu uticati na zaštitu informacija i informacionih sistema, sistem za zaštitu informacija će se neprekidno prilagođavati sprovođenjem novih bezbednosnih mera i procedura i putem poboljšanja već postojećih bezbednosnih mera i procedura. Dinamičko prilagođavanje bezbednosne politike u skladu sa zahtevima poslovanja i promenama od uticaja na početnu procenu rizika, je obaveza menadžera sigurnosti.

7. Upravljanje dokumentima u vezi sa zaštitom informacija

Dokumenta vezana za zaštitu informacija koje se štampaju u elektronskoj formi, a koja na taj način postaju dostupna svim zaposlenima i trećim licima, koja imaju pristup informacijama i informacionom sistemu kompanije. Svaki dokument vezan za zaštitu informacija mora da ima određenog čuvara koji je zadužen za njeno blagovremeno inoviranje i izmenu, kao i lice koje je nadležno za odobrenje dokumenta. Imena oba ta lica se ispisuju u donjem levom uglu dokumenta. U svakom dokumentu se naznačava datum njegovog stupanja na snagu.

Svaki zaposleni može da predloži izmenu i dopunu dokumenta tako što predlog prosleđuje čuvaru ili forumu za bezbednost. Čim se dokumenta izmene i odobre, moraju se objaviti bez odlaganja, i moraju se odmah obavestiti svi zaposleni u kompaniji i ona treća lica koja te izmene moraju uzeti u obzir u svom radu.

8. Sankcije

Svaki propust da se izvrši usaglašavanje sa pravilima zaštite informacija i odgovarajućim dokumentima smatra se povredom ugovora o radu i kao takav podleže sankcionisanju.