**\* OVO JE BESPLATNI OGLEDNI PREDLOŽAK DOKUMENTA \***

**Prilog 3 – Kontrolni popis za interni audit prema normi ISO 27001**

|  |  |  |  |
| --- | --- | --- | --- |
| Točka | Zahtjev norme | Usklađeno Da/Ne | Dokaz |
| 4.2 | Je li tvrtka odredila zainteresirane strane? |  |  |
| 4.2 | Postoji li popis svih zahtjeva zainteresiranih strana? |  |  |
| 4.3 | Je li opseg dokumentiran, s jasno definiranim granicama i sučeljima? |  |  |
| 5.1 | Je su li opći ciljevi ISMS-a u skladu sa strateškim smjerom? |  |  |
| 5.1 | Osigurava li uprava da ISMS ostvari svoje ciljeve? |  |  |
| 5.2 | Postoji li Politika informacijske sigurnosti s ciljevima ili okvirom za postavljanje ciljeva? |  |  |
| 5.2 | Jesu li zaposlenici unutar tvrtke upoznati s Politikom informacijske sigurnosti? |  |  |
| 5.3 | Jesu li uloge i odgovornosti za informacijsku sigurnost dodijeljene i priopćene? |  |  |
| 6.1.2 | Je li proces procjene rizika dokumentiran, uključujući i kriterije prihvatljivosti rizika i kriterije za procjenu rizika? |  |  |
| 6.1.2, 8.2 | Jesu li prepoznati rizici, njihovi vlasnici, vjerojatnost, posljedice i razina rizika; jesu li ti rezultati dokumentirani? |  |  |
| 6.1.3 | Je li proces obrade rizika dokumentiran, uključujući opcije obrade rizika? |  |  |
| 6.1.3, 8.3 | Jesu li obrađeni svi neprihvatljivi rizici koristeći opcije i mjere iz Aneksa A; jesu li ti rezultati dokumentirani? |  |  |
| 6.1.3 | Je li Izvješće o primjenjivosti izrađeno, s obrazloženjima i statusom za svaku sigurnosnu mjeru? |  |  |
| 6.1.3, 8.3 | Postoji li Plan obrade rizika odobren od strane vlasnika rizika? |  |  |
| 6.2 | Određuje li Plan obrade rizika tko je odgovoran za uvođenje koje mjere, s kojim resursima, koji su rokovi te koja se metoda procjene koristi? |  |  |
| 7.1 | Postoje li odgovarajući resursi za sve elemente ISMS-a? |  |  |
| 7.2 | Jesu li utvrđena potrebna znanja, provedene obuke i vode li se zapisi o stečenim znanjima? |  |  |
| 7.3 | Je li osoblje svjesno da postoji Politika informacijske sigurnosti, svoje uloge te posljedica nepridržavanja pravila? |  |  |
| 7.4 | Postoji li proces komunikacije povezan s informacijskom sigurnošću, uključujući odgovornosti i što je potrebno prenositi? |  |  |
| 7.5 | Postoji li postupak za upravljanje dokumentima i zapisima, uključujući tko pregledava i odobrava dokumente, gdje se i kako objavljuju, pohranjuju i štite? |  |  |
| 7.5 | Nadziru li se dokumenti vanjskog podrijetla? |  |  |
| 8.1 | Jesu li procesi koje izvode vanjski suradnici identificirani i nadzirani? |  |  |
| 9.1 | Je li utvrđeno što treba mjeriti, kojom metodom, tko je odgovoran, tko će analizirati i ocijeniti rezultate? |  |  |
| 9.1 | Jesu li rezultati mjerenja dokumentirani i prijavljeni odgovornim osobama? |  |  |
| 9.2 | Postoji li program audita koji definira vrijeme, odgovornosti, izvještavanje, kriterije za audit te opseg audita? |  |  |
| 9.2 | Jesu li interni auditi provedeni u skladu s programom audita, jesu li rezultati preneseni kroz interno izvješće o auditu i jesu li pokrenute relevantne popravne radnje? |  |  |
| 9.3 | Obavlja li uprava pregled redovito i jesu li rezultati dokumentirani u zapisniku sa sastanka? |  |  |
| 9.3 | Je li uprava odlučila o svim ključnim pitanjima važnim za uspjeh ISMS-a? |  |  |
| 10.1 | Reagira li tvrtka na svaku neusklađenost? |  |  |
| 10.1 | Razmatra li tvrtka uklanjanje uzroka neusklađenost i i poduzima li popravne radnje gdje je potrebno? |  |  |
| 10.1 | Jesu li sve neusklađenost i zabilježene, zajedno s popravnim radnjama? |  |  |
| A.5.1 | Jesu li sve potrebne Politike informacijske sigurnosti odobrene od strane uprave i jesu li objavljene? |  |  |
| A.5.1 | Jesu li sve Politike informacijske sigurnosti pregledane i ažurirane? |  |  |
| A.5.2 | Jesu li sve odgovornosti informacijske sigurnosti jasno definirane, kroz jedan ili više dokumenata? |  |  |
| A.5.3 | Jesu li dužnosti i odgovornosti utvrđene na takav način da se izbjegne sukob interesa, posebno s informacijama i sustavima gdje su uključeni visoki rizici? |  |  |
| A.5.4 | Zahtijeva li uprava, aktivno, da se svi zaposlenici i izvođači pridržavaju pravila informacijske sigurnosti? |  |  |
| A.5.5 | Je li jasno utvrđeno tko bi trebao biti u kontaktu s kojim državnim tijelima? |  |  |
| A.5.6 | Je li jasno utvrđeno tko bi trebao biti u kontaktu s posebnim interesnim skupinama ili strukovnim udrugama? |  |  |
| A.5.7 | Prikupljaju li se i analiziraju prijetnje informacijskoj sigurnosti kako bi se proizvela obavještajna informacija o prijetnjama? |  |  |
| A.5.8 | Jesu li pravila informacijske sigurnosti uključena u svaki projekt? |  |  |
| A.5.8 | Jesu li utvrđeni sigurnosni zahtjevi za nove informacijske sustave ili za bilo kakve promjene na njima? |  |  |
| A.5.9 | Izrađuje li se Popis resursa? |  |  |
| A.5.9 | Ima li svaki informacjski resurs u Popisu resursa određenog vlasnika? |  |  |
| A.5.10 | Jesu li pravila za odgovarajuće upravljanje informacijama i resursima dokumentirana? |  |  |
| A.5.10 | Postoje li procedure koje definiraju kako postupati s klasificiranim informacijama? |  |  |
| A.5.11 | Jesu li svi zaposlenici i izvođači vratili sve resurse u vlasništvu tvrtke nakon prestanka radnog odnosa? |  |  |
| A.5.12 | Jesu li informacije klasificirane prema određenim kriterijima? |  |  |
| A.5.13 | Jesu li klasificirane informacije označene u skladu s definiranim postupcima? |  |  |
| A.5.14 | Je li zaštita prijenosa informacija regulirana službenim politikama i procedurama? |  |  |
| A.5.14 | Postoje li ugovori s trećim stranama koji reguliraju sigurnost prijenosa informacija? |  |  |
| A.5.14 | Jesu li poruke koje se razmjenjuju putem mreža dobro zaštićene? |  |  |
| A.5.15 | Postoji li Politika kontrole pristupa koja definira poslovne i sigurnosne zahtjeve za kontrolu pristupa? |  |  |
| A.5.15 | Imaju li korisnici pristup samo onim mrežama i uslugama za koje su posebno ovlašteni? |  |  |
| A.5.16 | Jesu li prava pristupa osigurana formalnim postupkom registracije? |  |  |
| A.5.17 | Daju li se početne lozinke i drugi tajni podaci za provjeru autentičnosti na siguran način? |  |  |
| A.5.17 | Postoje li jasna pravila za korisnike o tome kako zaštititi lozinke i druge podatke za provjeru autentičnosti? |  |  |
| A.5.17 | Jesu li sustavi koji upravljaju lozinkama interaktivni i omogućuju li kreiranje sigurnih lozinki? |  |  |
| ***[ostatak redaka ne prikazuje se u ovom oglednom predlošku]*** | | | |
|  |  |  |  |

**\* ZAVRŠETAK OGLEDNOG PREDLOŠKA \***

(Kako biste pristupili potpunoj verziji dokumenta molimo Vas da kupite ISO 27001 paket dokumentacije <https://advisera.com/27001academy/hr/iso-27001-paket-dokumentacije/>)