**Kontrolni popis projekta implementacije ISO 27001**

|  |  |  |  |
| --- | --- | --- | --- |
| **Faze implementacije** | **Zadaci** | **Dokumenti iz paketa koji će se koristiti** | **Završeno** |
| *Pribavite podršku uprave* | Istražite koje bi prednosti norme ISO 27001 bile primjenjive na vašu tvrtku | - |  |
| Predstavite prednosti upravi i dobijte njihovu podršku | - |  |
| Dobijte službeno odobrenje za početak planiranja projekta | - |  |
|  |  |  |
| *Pripremite se za projekt* | Napišite politiku za kontrolu dokumenata | 01-01 Procedura za kontrolu dokumenata i zapisa |  |
| Podučite projektni tim | - |  |
| Napišite projektni plan, uključujući utvrđivanje upravitelja projekta, projektnog tima, sponzora projekta, potrebnih resursa i događaja | 02-01 Projektni plan |  |
| Navedite koje zainteresirane strane treba obavještavati o svakom koraku u projektu | - |  |
| Organizirajte prvi sastanak | - |  |
|  |  |  |
| *Identificirajte zahtjeve* | Propišite proceduru za identifikaciju zainteresiranih strana | 03-01 Procedura za identifikaciju zahtjeva |  |
| Identificirajte zahtjeve zainteresiranih strana | 03-02 Popis pravnih, regulatornih, ugovornih i drugih zahtjeva |  |
|  |  |  |
| *Utvrdite opseg, namjere uprave i odgovornosti* | Napišite dokument o opsegu ISMS-a | 04-01 Odluka o opsegu ISMS-a |  |
| Napišite Politiku informacijske sigurnosti | 05-01 Politika informacijske sigurnosti |  |
| Odlučite o ciljevima informacijske sigurnosti | 05-01 Politika informacijske sigurnosti |  |
|  |  |  |
| *Provedite upravljanje rizicima* | Razvijte metodologiju procjene rizika | 06-01 Metodologija za procjenu i obradu rizika |  |
| Provedite procjenu rizika | 06-02 Tablica procjene rizika |  |
| Provedite obradu rizika | 06-03 Tablica obrade rizika |  |
| Napišite Izvješće o procjeni i obradi rizika | 06-04 Izvješće o procjeni i obradi rizika |  |
|  |  |  |
| *Razvijte sigurnosni profil svoje tvrtke te akcijski plan kako to postići* | Izradite Izvješće o primjenjivosti | 07-01 Izvješće o primjenjivosti |  |
| Prihvatite preostale rizike | 07-01 Izvješće o primjenjivosti |  |
| Izradite Plan obrade rizika | 08-01 Plan obrade rizika |  |
|  |  |  |
| *Implementirajte sigurnosne mjere* | Provedite sve sigurnosne mjere propisane u Planu obrade rizika | Dokumenti u mapi "Sigurnosne mjere iz Aneksa A" |  |
| Održavajte zapise o implementaciji | Za ISMS dokumente to je vidljivo kroz povijest verzija dokumenta; za softver ovo bi mogao biti zapisnik o njegovom testiranju i izdavanju. |  |
|  |  |  |
| *Provedite programe obučavanja i osvješćivanja* | Provedite obuku za sve zaposlenike koji nemaju potrebne vještine | 10-01 Plan obučavanja i osvješćivanja |  |
| Provedite programe podizanja svijesti za sve zaposlenike i treće strane koje imaju ulogu u vašem ISMS-u | 10-01 Plan obučavanja i osvješćivanja |  |
|  |  |  |
| *Implementirajte procedure upravljanja* | Napišite proceduru za interni audit | 11-01 Procedura za interni audit |  |
| Izradite program audita | 11-02 Godišnji program internog audita |  |
| Propišite koja mjerenja u vezi s ciljevima za ISMS i za sigurnosne mjere treba izvesti | 12-01 Izvješće o mjerenju |  |
| Utvrdite izvore informacija koji će se koristiti u pregledu od strane uprave | 12-02 Zapisnik s pregleda od strane uprave |  |
| Napišite proceduru za popravnu radnju | 13-01 Procedura za popravnu radnju |  |
|  |  |  |
| *Upravljajte ISMS-om* | Održavajte sve zapise koje vaše vlastite politike i procedure zahtijevaju | Razni zapisi i dnevnici koji se stvaraju zbog ISMS dokumenata – npr. dnevnik izrade sigurnosne kopije (iz softvera za sigurnosno kopiranje), ispunjeni popis pravnih, regulatornih i ugovornih zahtjeva, itd. |  |
| Prema potrebi izvršite popravne radnje, kao posljedicu potrebnih poboljšanja u radu ISMS-a | 13-02 Obrazac za popravnu radnju |  |
|  |  |  |
| *Pratite i mjerite ISMS* | Obavezno pratite sve svoje sustave | Zapisi o praćenju utvrđeni u svakom implementiranom dokumentu, npr. broj incidenata, broj grešaka u pojedinom sustavu, itd. |  |
| Izmjerite jeste li postigli ciljeve postavljene za vaš ISMS i kontrole | 12-01 Izvješće o mjerenju |  |
|  |  |  |
| *Provedite interni audit* | Provedite interne audite | 11-04 Kontrolni popis za interni audit |  |
| Napišite izvješće o internom auditu | 11-03 Izvješće o internom auditu |  |
| Provedite popravne radnje kao posljedicu neusklađenosti utvrđenih tijekom internog audita | 13-02 Obrazac za popravnu radnju |  |
|  |  |  |
| *Provedite pregled od strane uprave* | Provedite pregled od strane uprave | - |  |
| Održavajte zapise s pregleda od strane uprave | 12-02 Zapisnik s pregleda od strane uprave |  |
| Provedite popravne radnje kao posljedicu poboljšanja utvrđenih tijekom pregleda od strane uprave | 13-02 Obrazac za popravnu radnju |  |
|  |  |  |
| *Certifikacijski audit* | Pribavite ponude od nekoliko certifikacijskih tijela | - |  |
| Odaberite certifikacijsko tijelo | - |  |
| 1. faza certifikacijskog audita | - |  |
| 2. faza certifikacijskog audita | - |  |
| Nadzorni posjeti | - |  |
|  |  |  |