

ISO 27001 Paket dokumentacije

Napomene: dokumentaciju je najbolje implementirati redoslijedom kojim je navedena u ovom popisu. Redoslijed implementacije dokumentacije vezane za Aneks A se određuje kroz Plan obrade rizika.

<i>Broj u paketu</i>	<i>Naziv dokumenta</i>	<i>Sukladan točkama norme</i>	<i>Dokument je obavezan po ISO 27001</i>
0.	Procedura za upravljanje dokumentacijom i zapisima	ISO/IEC 27001 7.5	
1.	Projektni plan		
2.	Procedura za identifikaciju zahtjeva	ISO/IEC 27001 4.2 i A.18.1.1	
2.1.	Prilog – Popis pravnih, regulatornih, ugovornih i ostalih zahtjeva	ISO/IEC 27001 4.2 i A.18.1.1	✓*
3.	Odluka o opsegu ISMS-a	ISO/IEC 27001 4.3	✓
4.	Politika informacijske sigurnosti	ISO/IEC 27001 5.2 i 5.3	✓
5.	Metodologija za procjenu i obradu rizika	ISO/IEC 27001 6.1.2, 6.1.3, 8.2 i 8.3	✓
5.1.	Prilog 1 – Tablica procjene rizika	ISO/IEC 27001 6.1.2 i 8.2	✓
5.2.	Prilog 2 – Tablica obrade rizika	ISO/IEC 27001 6.1.3 i 8.3	✓
5.3.	Prilog 3 – Izvješće o procjeni i obradi rizika	ISO/IEC 27001 8.2 i 8.3	✓
6.	Izvješće o primjenjivosti	ISO/IEC 27001 6.1.3 d)	✓
7.	Plan obrade rizika	ISO/IEC 27001 6.1.3, 6.2 i 8.3	✓
8.	(Aneks A – kontrole)		
8. A.6	Politika korištenja vlastitih uređaja (BYOD)	ISO/IEC 27001 A.6.2.1, A.6.2.2, A.13.2.1	
8.	Politika mobilnih uređaja i rada	ISO/IEC 27001 A.6.2	

Broj u paketu	Naziv dokumenta	Sukladan točkama norme	Dokument je obavezan po ISO 27001
A.6	na daljinu	A.11.2.6	
8. A.7	Izjava o povjerljivosti	ISO/IEC 27001 A.7.1.2, A.13.2.4, A.15.1.2	✓*
8. A.7	Izjava o prihvaćanju dokumenata ISMS-a	ISO/IEC 27001 A.7.1.2	✓*
8. A.8	Popis resursa	ISO/IEC 27001 A.8.1.1, A.8.1.2	✓*
8. A.8	Politika pravilne uporabe	ISO/IEC 27001 A.6.2.1, A.6.2.2, A.8.1.2, A.8.1.3, A.8.1.4, A.9.3.1, A.11.2.5, A.11.2.6, A.11.2.8, A.11.2.9, A.12.2.1, A.12.3.1, A.12.5.1, A.12.6.2, A.13.2.3, A.18.1.2	✓*
8. A.8	Politika klasifikacije informacija	ISO/IEC 27001 A.8.2.1, A.8.2.2, A.8.2.3, A.8.3.1, A.8.3.3, A.9.4.1, A.13.2.3	
8. A.9	Politika kontrole pristupa	ISO/IEC 27001 A.9.1.1, A.9.1.2, A.9.2.1, A.9.2.2, A.9.2.3, A.9.2.4, A.9.2.5, A.9.2.6, A.9.3.1, A.9.4.1, A.9.4.3	✓*
8. A.9	Politika uporabe lozinki (napomena: može biti implementirana kao dio Politike kontrole pristupa)	ISO/IEC 27001 A.9.2.1, A.9.2.2, A.9.2.4, A.9.3.1, A.9.4.3	
8. A.10	Politika uporabe kriptografskih kontrola	ISO/IEC 27001 A.10.1.1, A.10.1.2, A.18.1.5	
8. A.11	Politika čistog stola i čistog ekrana (napomena: može biti implementirana kao dio Politike pravilne uporabe)	ISO/IEC 27001 A.11.2.8, A.11.2.9	
8. A.11	Politika uklanjanja i uništavanja (napomena: može biti	ISO/IEC 27001 A.8.3.2, A.11.2.7	

Broj u paketu	Naziv dokumenta	Sukladan točkama norme	Dokument je obavezan po ISO 27001
	implementirana kao dio Operativnih procedura za informacijsku i komunikacijsku tehnologiju)		
8. A.11	Procedure za rad u sigurnim područjima	ISO/IEC 27001 A.11.1.5	
8. A.12	Operativne procedure za informacijsku i komunikacijsku tehnologiju	ISO/IEC 27001 A.8.3.2, A.11.2.7, A.12.1.1, A.12.1.2, A.12.3.1, A.12.4.1, A.12.4.3, A.13.1.1, A.13.1.2, A.13.2.1, A.13.2.2, A.14.2.4	✔ *
8. A.12	Politika upravljanja promjenama (napomena: može biti implementirana kao dio Operativnih procedura za informacijsku i komunikacijsku tehnologiju)	ISO/IEC 27001 A.12.1.2, A.14.2.4	
8. A.12	Politika sigurnosnih kopija (napomena: Može biti implementirana kao dio Operativnih procedura za informacijsku i komunikacijsku tehnologiju)	ISO/IEC 27001 A.12.3.1	
8. A.13	Politika prijenosa informacija (napomena: Može biti implementirana kao dio Operativnih procedura za informacijsku i komunikacijsku tehnologiju)	ISO/IEC 27001 A.13.2.1, A.13.2.2	
8. A.14	Politika sigurnog razvoja	ISO/IEC 27001 A.14.1.2, A.14.1.3, A.14.2.1, A.14.2.2, A.14.2.5, A.14.2.6, A.14.2.7, A.14.2.8, A.14.2.9, A.14.3.1	✔ *
8.	Prilog – Specifikacija zahtjeva za	ISO/IEC 27001 A.14.1.1	✔ *

Broj u paketu	Naziv dokumenta	Sukladan točkama norme	Dokument je obavezan po ISO 27001
A.14	informacijski sustav		
8. A.15	Politika sigurnosti dobavljača	ISO/IEC 27001 A.7.1.1, A.7.1.2, A.7.2.2, A.8.1.4, A.14.2.7, A.15.1.1, A.15.1.2, A.15.1.3, A.15.2.1, A.15.2.2	
8. A.15	Prilog – Sigurnosne klauzule za dobavljače i partnere	ISO/IEC 27001 A.7.1.2, A.14.2.7, A.15.1.2, A.15.1.3	✓*
8. A.16	Procedura za upravljanje incidentima	ISO/IEC 27001 A.7.2.3, A.16.1.1, A.6.1.2, A.16.1.3, A.16.1.4, A.16.1.5, A.16.1.6, A.16.1.7	✓*
8. A.16	Prilog – Jedinstveni popis incidenata	ISO/IEC 27001 A.16.1.6	
8. A.17	Plan oporavka od havarije	ISO/IEC 27001 A.17.1.2	✓*
9.	Plan obučavanja i osvježavanja	ISO/IEC 27001 7.2, 7.3	✓
10.	Procedura za interni audit	ISO/IEC 27001 9.2	
10.1.	Prilog 1 – Godišnji plan internih audita	ISO/IEC 27001 9.2	✓
10.2.	Prilog 2 – Izvješće o internom auditu	ISO/IEC 27001 9.2	✓
10.3.	Prilog 3 – Kontrolni popis za interni audit	ISO/IEC 27001 9.2	
11.	Zapisnik sa pregleda od strane menadžmenta	ISO/IEC 27001 9.3	✓
12.	Procedura za korektivne mjere	ISO/IEC 27001 10.1	
12.1.	Prilog – Obrazac za korektivnu mjeru	ISO/IEC 27001 10.1	✓

*Navedeni dokumenti su obvezni jedino ako su kontrole kojima pripadaju propisane kao primjenjive kroz Izvješće o primjenjivosti

Za pomoć oko ispunjavanja ovih dokumenata pogledajte:

- 1) Našu seriju video tutorijala <http://www.iso27001standard.com/hr/tutorials/>
- 2) Našu seriju webinarara <http://www.iso27001standard.com/hr/webinars/>