



ISO 27001 paket dokumentacije

<https://advisera.com/27001academy/hr/iso-27001-paket-dokumentacije/>

Napomena: Ako je moguće, dokumentaciju bi trebalo implementirati redoslijedom kojim je ovdje navedena. Redoslijed implementacije dokumentacije vezane uz Aneks A definiran je Planom obrade rizika.

Br.	Oznaka dokumenta	Naziv dokumenta	Relevantne točke / mjere u ISO 27001	Obavezno prema ISO 27001
	01	Upravljanje dokumentima		
1	01	Procedura za upravljanje dokumentima i zapisima	7.5; A.5.33	
	02	Pripreme za projekt		
2	01	Projektni plan		
	03	Identifikacija zahtjeva		
3	01	Procedura za identifikaciju zahtjeva	4.2; A.5.31	
4	02	Prilog 1 – Popis pravnih, regulatornih, ugovornih i ostalih zahtjeva	4.2; A.5.29; A.5.31	✓ *
	04	Opseg ISMS-a		
5	01	Odluka o opsegu ISMS-a	4.3	✓
	05	Okvirne politike		
6	01	Politika informacijske sigurnosti	5.2; 5.3**; 6.2; 7.4; A.6.3	✓
	06	Procjena i obrada rizika		
7	01	Metodologija za procjenu i obradu rizika	6.1.2; 6.1.3; 8.2; 8.3	✓
8	02	Prilog 1 – Tablica procjene rizika	6.1.2; 8.2	✓
9	03	Prilog 2 – Tablica obrade rizika	6.1.3; 8.3	✓
10	04	Prilog 3 – Izvješće o procjeni i obradi rizika	8.2; 8.3	✓

Br.	Oznaka dokumenta	Naziv dokumenta	Relevantne točke / mjere u ISO 27001	Obavezno prema ISO 27001
	07	Primjenjivost mjera		
11	01	Izvešće o primjenjivosti	6.1.3 d)	✓
	08	Plan implementacije		
12	01	Plan obrade rizika	6.1.3; 6.2; 7.1; 8.3; 9.1	✓
	09	Sigurnosne mjere iz Aneksa A		
13	01	Politika sigurnosti informacijskog sustava	A.5.9; A.5.10; A.5.11; A.5.14; A.5.17; A.5.32; A.6.7; A.7.7; A.7.9; A.7.10; A.8.1; A.8.7; A.8.10; A.8.12; A.8.13; A.8.19; A.8.23	✓ *
14	02	Politika čistog stola i čistog ekrana (Napomena: ovo se može implementirati kao dio Politike sigurnosti informacijskog sustava.)	A.7.7; A.8.1	
15	03	Politika mobilnih uređaja, rada na daljinu i rada od kuće (Napomena: ovo se može implementirati kao dio Politike sigurnosti informacijskog sustava.)	A.6.7; A.7.9; A.8.1	
16	04	Politika korištenja vlastitih uređaja (BYOD)	A.5.14; A.6.7; A.8.1	
17	05	Procedure za rad u sigurnim područjima	A.7.4; A.7.6	
18	06	Politika klasifikacije informacija	A.5.9; A.5.10; A.5.12; A.5.13; A.5.14; A.7.10; A.8.3; A.8.5; A.8.11; A.8.12	✓ *
19	07	Popis resursa	A.5.9	✓ *

Br.	Oznaka dokumenta	Naziv dokumenta	Relevantne točke / mjere u ISO 27001	Obavezno prema ISO 27001
20	08	Sigurnosne procedure za IT odjel	A.5.7; A.5.14; A.5.37; A.7.10; A.7.14; A.8.4; A.8.6; A.8.7; A.8.8; A.8.9; A.8.10; A.8.12; A.8.13; A.8.15; A.8.16; A.8.17; A.8.18; A.8.20; A.8.21; A.8.22; A.8.23; A.8.31; A.8.32	 *
21	09	Politika upravljanja promjenama (Napomena: ovo se može implementirati kao dio Sigurnosnih procedura za IT odjel.)	A.8.32	
22	10	Politika sigurnosnih kopija (Napomena: ovo se može implementirati kao dio Sigurnosnih procedura za IT odjel.)	A.8.13	
23	11	Politika prijenosa informacija (Napomena: ovo se može implementirati kao dio Sigurnosnih procedura za IT odjel.)	A.5.14	
24	12	Politika odlaganja i uništavanja (Napomena: ovo se može implementirati kao dio Sigurnosnih procedura za IT odjel.)	A.7.10; A.7.14; A.8.10	
25	13	Politika o uporabi šifriranja	A.5.31; A.8.24	
26	14	Politika kontrole pristupa	A.5.15; A.5.16; A.5.17; A.5.18; A.8.2; A.8.3; A.8.4; A.8.5; A.8.11	
27	15	Politika uporabe lozinki (Napomena: Ovo se može implementirati kao dio Politike kontrole pristupa.)	A.5.16; A.5.17; A.5.18	
28	16	Politika sigurnog razvoja	A.5.33; A.8.11; A.8.25; A.8.26; A.8.27; A.8.28; A.8.29; A.8.30; A.8.31; A.8.32; A.8.33	 *

Br.	Oznaka dokumenta	Naziv dokumenta	Relevantne točke / mjere u ISO 27001	Obavezno prema ISO 27001
29	17	Prilog 1 – Specifikacija zahtjeva za informacijski sustav	A.8.26	
30	18	Politika sigurnosti dobavljača	A.5.7; A.5.11; A.5.19; A.5.20; A.5.21; A.5.22; A.5.23; A.6.1; A.6.2; A.6.3; A.8.30	
31	19	Sigurnosne klauzule za dobavljače i partnere	A.5.20; A.5.21; A.6.2; A.8.30	
32	20	Procedura za upravljanje incidentima	7.4; A.5.7; A.5.24; A.5.25; A.5.26; A.5.27; A.5.28; A.6.4; A.6.8	✓ *
33	21	Prilog 1 – Dnevnik incidenata	A.5.27	
34	22	Plan oporavka od katastrofe	7.4; A.5.29; A.5.30; A.8.14	
35	23	Izjava o povjerljivosti	A.5.20; A.6.2; A.6.5; A.6.6	✓ *
36	24	Izjava o prihvatanju dokumenata ISMS-a	A.6.2	
	10	Obuka i podizanje svijesti		
37	01	Plan obučavanja i osvještavanja	7.2; 7.3; 7.4; A.6.3	✓
	11	Interni audit		
38	01	Procedura za interni audit	9.2; A.5.30; A.5.35; A.8.34	
39	02	Prilog 1 – Godišnji program internog audita	9.2	✓
40	03	Prilog 2 – Izvješće o internom auditu	9.2	✓
41	04	Prilog 3 – Kontrolni popis za interni audit	9.2	
	12	Pregled od strane uprave		

<i>Br.</i>	<i>Oznaka dokumenta</i>	<i>Naziv dokumenta</i>	<i>Relevantne točke / mjere u ISO 27001</i>	<i>Obavezno prema ISO 27001</i>
42	01	Izvešće o mjerenju	6.2; 9.1	✓
43	02	Zapisnik s pregleda od strane uprave	9.3	✓
	13	Popravne radnje		
44	01	Procedura za popravnu radnju	10.1; A.5.27	
45	02	Prilog 1 – Obrazac za popravnu radnju	10.1; 10.2	✓

*Navedeni dokumenti obavezni su samo ako su odgovarajuće kontrole identificirane kao primjenjive u Izjavi o primjenjivosti.

**Opće uloge i odgovornosti opisane su u Politici informacijske sigurnosti, dok su detaljne uloge i odgovornosti navedene u svakom dokumentu ovog Paketa.