

OBR-1: Popis vzpostavljenih kontrol informacijske varnosti pri izvajalcu

	Opis kontrole	Kontrola vzpostavljena	
	Ime podjetja:		
	1. Politika varovanja informacij		
1.1	V podjetju obstaja dokumentirana politika varovanja informacij.	Da	Ne
1.2	Pri pripravi varnostne politike se upošteva poslovne zahteve, relevantno zakonodajo in predpise s področja delovanja podjetja.	Da	Ne
1.3	Politika varovanja informacij se redno dokumentirano pregleduje in po potrebi posodablja.	Da	Ne
1.4	S politiko varovanja informacij in njenimi spremembami so seznanjeni vsi zaposleni in jim je ta ves čas zaposlitve razpoložljiva.	Da	Ne
	2. Analiza in upravljanje informacijskih in drugih tveganj		
2.1	V podjetju je bila izvedena in dokumentirana analiza tveganj.	Da	Ne
2.2	Analiza tveganj se posodablja najmanj enkrat letno.	Da	Ne
2.3	Z rezultati analize tveganja se seznani direktor podjetja.	Da	Ne
	3. Ravnanje z viri informacijske tehnologije		
3.1	V podjetju obstaja dokumentirana politika uporabe virov informacijske tehnologije.	Da	Ne
3.2	V podjetju je opravljen popis vseh informacijskih virov, ki so del njegovega informacijskega sistema.	Da	Ne
3.3	Vsi informacijski viri imajo določene lastnike/skrbnike, ki so seznanjeni s svojimi odgovornostmi.	Da	Ne
3.4	V podjetju je opredeljen postopek, ki zagotavlja, da zaposleni ob prenehanju opravljanja dela vse vire informacijske tehnologije vrnejo podjetju.	Da	Ne
3.5	V podjetju je opredeljena politika uporabe in ravnanja z izmenljivimi nosilci podatkov.	Da	Ne

	4. Sistem upravljanja incidentov	
4.1	V podjetju je vzpostavljeno sistematično zaznavanje in dokumentiranje dogodkov, ki imajo vpliv na varnost poslovanja.	Da Ne
4.2	Zaznane dogodke se razvršča po kritičnosti vpliva na poslovanje.	Da Ne
4.3	Zaznane in dokumentirane dogodke se sistematično pregleduje in analizira.	Da Ne
4.4	Na podlagi obravnave zaznanih in dokumentiranih dogodkov se določi in izvede ustrezne ukrepe.	Da Ne
	5. Načrt neprekinjenega poslovanja	
5.1	Podjetje razpolaga z dokumentiranim načrtom neprekinjenega poslovanja.	Da Ne
5.2	Vloge in odgovornosti za izvedbo načrta neprekinjenega poslovanja so opredeljene in dokumentirane.	Da Ne
5.3	Podjetje razpolaga z rezervno lokacijo.	Da Ne
5.4	Načrt neprekinjenega poslovanja se redno preizkuša, to dokumentira in na tej podlagi načrt posodablja.	Da Ne
	6. Ozaveščanje o informacijski varnosti	
6.1	V podjetju se izvaja dokumentirano ozaveščanje in izobraževanje o varnosti informacij in o načrtu neprekinjenega poslovanja.	Da Ne
6.2	Vsaj ena oseba iz podjetja se redno udeležuje zunanjih izobraževanj s področja varovanja informacij.	Da Ne
6.3	Ob zaposlovanju novih oseb so vzpostavljene varnostne kontrole.	Da Ne
	7. Varovalni ukrepi v okviru informacijske tehnologije	
7.1	V podjetju so uvedeni ukrepi za potrebe varovanja informacij v okviru informacijske tehnologije na različnih področjih, ki temeljijo na analizi tveganj.	Da Ne
7.2	V podjetju je uveden dokumentiran sistem upravljanja sprememb v okviru informacijske tehnologije.	Da Ne

7.3	Vzpostavljeni so dokumentirani postopki preprečevanja odtekanja informacij.	Da	Ne
7.4	Za ugotavljanje varnostnih pomanjkljivosti in sprejetja ustreznih tehničnih varovalnih ukrepov, se v sodelovanju z zunanjim neodvisnim izvajalcem opravlja teste ranljivosti.	Da	Ne
7.5	V podjetju se opravljajo pregledi izvajanja ukrepov varovanja.	Da	Ne
8. Temeljna nadzorstva za zagotavljanje informacijske varnosti			
8.1	V podjetju so uvedena naslednja področja varovanja (možnih je več spodnjih odgovorov):		
	fizična varnost in nadzor dostopa	Da	Ne
	alarm s prenosom na varnostno službo	Da	Ne
	videonadzor	Da	Ne
	protipožarna zaščita	Da	Ne
	fizično varovanje papirne dokumentacije	Da	Ne
	zaščita pred izpadom električne energije	Da	Ne
	požarni zid pred zunanjim omrežjem	Da	Ne
	protivirusna zaščita	Da	Ne
	omejitev vnosa in uporabe zasebnih mobilnih naprav za službene potrebe	Da	Ne
	nadzor oddaljenega dela in dostopa do omrežja	Da	Ne
	klasifikacija informacij po zaupnosti	Da	Ne
	uporaba načela čiste mize in čistega zaslona	Da	Ne
	logična kontrola dostopa in zaščita v okviru informacijske tehnologije	Da	Ne
	uporaba šifriranja	Da	Ne
	ločeno razvojno, testno in produkcijsko okolje	Da	Ne
	revizijska sled uporabe ključnih informacijskih sredstev	Da	Ne
	varnostno kopiranje	Da	Ne

8.2	V podjetju se redno spremlja dogodke na sistemih in druge dogodke, ki lahko predstavljajo incidente.	Da	Ne
9. Procesna ureditev			
9.1	Poslovni procesi podjetja so dokumentirani.	Da	Ne
9.2	Pojetje ima veljaven certifikat za sistem vodenja (možnih je več odgovorov):		
	po standardu ISO/IEC 9001	Da	Ne
	po standardu ISO/IEC 27001	Da	Ne
	po drugem standardu za procesno vodenje	Da	Ne
9.3	Seznanitev zaposlenih s postopki varovanja informacij v podjetju je dokumentirana.	Da	Ne
9.4	Zaposleni ob začetku opravljanja dela podpišejo izjavo o varovanju poslovne skrivnosti.	Da	Ne
9.5	Vsi projekti, ki se vodijo v podjetju, se na določeni točki varnostno ocenijo.	Da	Ne

Podpis odgovorne osebe izvajalca:

OBR-2: Seznam osebja izvajalca, ki ima pri vzdrževanju programske rešitve dostop do informacijskih sistemov in informacij naročnika

Naziv izvajalca: _____

Naziv naročnika: _____

Zap.št.	Ime in priimek	Kontaktne podatki	Vloga pri izvajalcu
1			
2			
3			
4			
5			
6			
7			
8			
9			
10			

Podpis odgovorne osebe izvajalca:

OBR-3: Opis naročnikovih informacij, do katerih osebje izvajalca pri vzdrževanju programske rešitve dostopa

Naziv izvajalca: _____

Naziv naročnika: _____

Zap.št.	Naziv informacij	Vsebina informacij	Način dostopa do informacij
1			
2			
3			
4			
5			
6			
7			
8			
9			
10			
11			
12			
13			
14			
15			

Podpis odgovorne osebe izvajalca: