Vprašalnik metodologije za vrednotenje stanja informacijske varnosti pri ponudniku

IKT - Vprašalnik metodologije za vrednotenje stanja informacijske varnosti		Izpolni / obkroži ponudnik	Največje možno število točk v primeru odgovora "da"
			105
	Ime podjetja ponudnika:		
	Okvirno število zaposlenih:		
	Kraj in datum izpolnjevanja:		
	Ime odgovorne osebe:		
	Podpis odgovorne osebe:		
	1. Politika varovanja informacij		
1.1.	Ali obstaja v vaši organizacij dokumentirana politika varovanja informacij?	Da Ne	3
1.2.	Ali ste pri pripravi varnostne politike upoštevali poslovne zahteve, relevantno zakonodajo in predpise s področja delovanja vaše organizacije in jih vanjo zapisali?	Da Ne	1
1.3.	Ali dokumentirano politiko varovanja informacij odobrava direktor družbe oziroma član najvišjega vodstva?	Da Ne	1
1.4.	Ali redno pregledujete in po potrebi posodabljate dokumentirano politiko varovanja informacij?	Da Ne	2
1.5.	Ali so s politiko varovanja informacij in njenimi spremembami seznanjeni vsi zaposleni in jim je ta ves čas zaposlitve razpoložljiva?	Da Ne	2
1.6.	Ali je bila varnostna politika kdaj pregledana s strani neodvisnih strokovnjakov?	Da Ne	1
	2. Analiza in upravljanje informacijskih in drugih tveganj		
2.1.	Ali je bila v vaši organizaciji izvedena in dokumentirana analiza tveganj?	Da Ne	3
2.2.	V kakšnem obsegu se izvaja analiza tveganj?	v celotni organizaciji (2 točki)	skupaj največ 2

		/ samo v nekaterih delih organizacije (1 točki) / analiza tveganj se ne izvaja (0 točk)	
2.3.	Ali se izvaja oziroma posodablja analiza tveganj najmanj enkrat letno?	Da Ne	2
2.4.	Ali se z rezultati analize tveganja seznani direktor družbe oziroma člani najvišjega vodstva?	Da Ne	1
	3. Ravnanje z viri informacijske tehnologije		
3.1.	Ali imate v vaši organizaciji dokumentirano politiko uporabe virov informacijske tehnologije?	Da Ne	3
3.2.	Ali imate opravljen popis vseh informacijskih virov, ki so del informacijskega sistema podjetja?	Da Ne	2
3.3.	Ali imajo vsi informacijski viri določene lastnike/skrbnike in so ti seznanjeni s svojimi odgovornostmi?	Da Ne	1
3.4.	Ali je v organizaciji opredeljen točen postopek, ki zagotavlja, da zaposleni in zunanji izvajalci ob prenehanju opravljanj dela, vse vire informacijske tehnologije vrnejo organizaciji?	Da Ne	2
3.5.	Ali imate v organizaciji opredeljeno politiko uporabe in ravnanja z zunanjimi nosilci podatkov?	Da Ne	2
	4. Obstoj sistema upravljanja incidentov		
4.1.	Ali v vaši organizaciji sistematično zaznavate in dokumentirate dogodke, ki imajo vpliv na varnost poslovanja in poslovanja na sploh?	Da Ne	3
4.2.	Ali zaznane dogodke razvrščate po kritičnosti vpliva na poslovanje?	Da Ne	1
4.3.	Ali sistematično pregledujete in analizirate zaznane in dokumentirane dogodke?	Da Ne	2
4.4.	Ali na podlagi obravnave zaznanih in dokumentiranih dogodkov sprejmete ustrezne sklepe in jih izvedete?	Da Ne	2
	5. Obstoj načrtov neprekinjenega poslovanja in njihova vsebina		
5.1.	Ali imate v vaši organizaciji dokumentirane načrte neprekinjenega poslovanja?	Da Ne	3
5.2.	Za katera poslovna področja velja načrt neprekinjenega poslovanja?		skupaj največ 2

		za vsa poslovna področja (2 točki) / za ključna poslovna področja, ki zagotavljajo delovanje podjetja (1 točka) / nimamo načrtov neprekinjenega poslovanja (0 točk)	
5.3.	Ali imate opredeljeno in dokumentirane vloge in odgovornosti za izvedbo narta neprekinjenega poslovanja (to niso položaji in funkcije iz rednih poslovnih procesov)?	Da Ne	1
5.4.	Rezervna lokacija: (možnih je več odgovorov)		skupaj največ 2
	je opremljena z vso potrebno IT infrastrukturo in drugimi viri, ki sledijo iz ustreznih analiz	Da Ne	1
	ima opremljena delovna mesta za zaposlene in opremljene prostore za vodstvo	Da Ne	1
	ni določena in ne obstaja	Da Ne	1
5.5.	Ali načrte neprekinjenega poslovanja redno preizkušate, to dokumentirate in na tej podlagi načrte posodabljate?	Da Ne	2
	6. Obstoj programa ozaveščanja o informacijski varnosti		
6.1.	Ali v vaši organizaciji izvajate dokumentirana ozaveščanja in izobraževanja o varnosti informacij in načrtu neprekinjenega poslovanja?	Da Ne	3
6.2.	Ali se vsaj ena oseba v vaši organizaciji redno udeležuje zunanjih izobraževanj s področja varovanja informacij?	Da Ne	1
6.3.	Ali ozaveščanje o varnosti informacij opravite za vse zaposlene, ki opravljajo delo v vaši organizaciji	Da Ne	2
6.4.	Ali kdaj uporabljate zunanjega izvajalca, da izvede program ozaveščanja ali izobraževanja o informacijski varnosti ali načrtovanju neprekinjenega poslovanja?	Da Ne	1
6.5.	Ali ste kdaj ob izrednem dogodku večjega vpliva na poslovanje pri vas organizirali dokumentirano ozaveščanje o dogodku, da se podobno ne bi več pripetilo?	Da Ne	2
6.6.	Ali imate ob zaposlovanju novih oseb vzpostavljene varnostne kontrole?	Da Ne	1

	7. Uvedeni varovalni ukrepi v okviru informacijske tehnologije		
7.1.	Ali imate v organizacij sistematično uvedene ukrepe za potrebe varovanja informacij v okviru informacijske tehnologije na različnih področjih, ki temeljijo na analizi tveganj vašega poslovnega okolja?	Da Ne	2
7.2.	Ali imate uveden dokumentiran sistem upravljanja sprememb v okviru informacijske tehnologije?	Da Ne	2
7.3.	Vaša dokumentacija o informacijskih sistemih vsebuje (možnih je več odgovorov):		skupaj največ 3
	načrt razvoja informacijskega sistema	Da Ne	1
	načrt razvoja kapacitet sistemov	Da Ne	1
	postopke sprejemanja sistemov v produkcijo	Da Ne	1
7.4.	Ali imate vzpostavljene dokumentirane postopke preprečevanja odtekanja informacij?	Da Ne	2
7.5.	Ali za ugotavljanje varnostnih pomanjkljivosti in sprejetja ustreznih tehničnih varovalnih ukrepov, v sodelovanju z zunanjimi neodvisnim izvajalcem, izvajate teste ranljivosti?	Da Ne	2
7.6.	Ali izvajate preglede izvajanja ukrepov varovanja?	za vse ukrepe izvajamo notranje in zunanje preglede (2 točki) / za vse ukrepe izvajamo samo notranje preglede (2 točki) / preglede izvajamo samo za pomembnejše ukrepe (0 točk) / ne izvajamo pregledov (0 točk)	skupaj največ 2
	8. Temeljni ukrepi varovanja		
8.1.	Katera področja varovanja ste uvedli v podjetju? (možnih je več spodnjih odgovorov)		skupaj največ 18
	fizična varnost in nadzor dostopa	Da Ne	1

	alarm s prenosom na varnostno službo	Da Ne	1
	Videonadzor	Da Ne	1
	protipožarna zaščita	Da Ne	1
	fizično varovanje papirne dokumentacije	Da Ne	1
	zaščita pred izpadom električne energije	Da Ne	1
	požarni zid pred zunanjim omrežjem	Da Ne	1
	proti-virusna zaščita	Da Ne	1
	omejitev vnosa in uporabe mobilnih naprav za službene potrebe	Da Ne	1
	nadzor oddaljenega dela in dostopa do omrežja	Da Ne	1
	klasifikacija informacij po zaupnosti	Da Ne	1
	uporaba načela čiste mize in čistega zaslona	Da Ne	1
	logična kontrola dostopa in zaščita v okviru informacijske tehnologije	Da Ne	1
	uporaba šifriranja	Da Ne	1
	ločeno razvojno, testno in produkcijsko okolje	Da Ne	1
	revizijsko sled za ključna informacijska sredstva	Da Ne	1
	varnostno kopiranje	Da Ne	1
	upoštevanje zakonodaje (predvsem zakon, ki ureja varstvo osebnih podatkov in zakon, ki ureja elektronsko poslovanje in elektronski podpis)	Da Ne	1
8.2.	V toku izvajanja procesov varovanja se ustvarijo zapisi in dokazi o njihovem izvajanju. Ali lahko na ta način pokažete, da ukrepe res izvajate?	da, za vse procese in ukrepe (2 točki) /delno (1 točka) /ne (0 točk)	skupaj največ 2
8.3.	Ali v podjetju redno spremljate dogodke na sistemih in druge dogodke, ki lahko predstavljajo incidente?	da, sistemi se stalno spremljajo (24/7) (2 točki) / da, sistemi se spremljajo med	skupaj največ 2

		delovnim časom (1 točka) / dogodkov ne spremljamo redno (0 točk)	
8.4.	Ali podjetje načrtuje posebna sredstva za področje varovanja informacij?	Da Ne	2
	9. Procesna ureditev in disciplina		
9.1.	Ali imate v organizaciji dokumentirane poslovne procese?	Da Ne	2
9.2.	Ali imate v organizaciji veljaven certifikat za sistem vodenja? (možnih je več odgovorov)		skupaj največ 5
	da, po standardu ISO 9001	Da Ne	1
	da, po standardu ISO/IEC 27001	Da Ne	2
	da, po standardu BS 25999	Da Ne	1
	da, po branžnem ali drugem standardu za procesno vodenje	Da Ne	1
9.3.	Ali imate dokumentirano, da so zaposleni seznanjeni s postopki in nivojem varovanja informacij v vaši organizaciji?	Da Ne	1
9.4.	Ali ste reden plačnik in svoje obveznosti do zaposlenih, zunanjih izvajalcev in dobaviteljev izpolnjujete brez zamud?	Da Ne	1
9.5.	Ali vsi zaposleni ob začetku opravljanja dela in izvajalci ter podizvajalci podpišejo izjavo o varovanju poslovne skrivnosti?	Da Ne	2
9.6.	Ali so vsi projekti, ki se vodijo v vašem podjetju na določeni točki varnostno ocenjeni oziroma potrjeni s strani osebe za varovanje informacij?	Da Ne	1

Elektronsko oddani obrazec v informacijskem sistemu e-JN se šteje za datiranega in podpisanega s strani ponudnikove odgovorne osebe in je tako zavezujoč za ponudnika v razmerju do naročnika.