

Podatki ponudnika
Ime podjetja:

Kontaktna oseba (ime, funkcija, e-naslov,
telefon):



Varnostni vprašalnik: Upravljanje dobaviteljske verige

Upravljanje		
1.1	Ali obstaja v vaši organizaciji vloga ali skupina, ki je končno odgovorna za upravljanje informacijske varnosti? Prosimo, navedite podrobnosti.	
1.2	Ali imate objavljeno politiko informacijske varnosti, ki jo je odobrilo višje vodstvo? Če je odgovor »da«, prosimo, da predložite kopijo.	
1.3	Ali imate politiko upravljanja tveganj, ki vključuje določbe za informacijsko varnost?	
1.4	Ali redno ocenjujete tveganja informacijske varnosti in sprejemate ukrepe za ublažitev ugotovljenih tveganj? Če je tako, opišite postopek in navedite datum zadnje ocene.	
1.5	Ali so bili v vaši organizaciji opravljeni kakšni neodvisni varnostni pregledi/revizije tretjih oseb? Če so bili, prosimo, navedite, kdo je opravil	



	revizijo/pregled, in datum zadnje izvedbe.	
1.6	Ali vaša organizacija usklajuje svoj sistem upravljanja informacijske varnosti s katerim koli industrijskim okvirom/standardom? Npr. CSA CCM, NIST CSF, ISO27001. Prosimo, navedite podrobnosti.	
1.7	Ali ima vaša organizacija kakršne koli certifikate za informacijsko varnost, kot je ISO 27001? Če jih ima, navedite podrobnosti o obsegu in datumu poteka veljavnosti certifikata.	
1.8	Ali ste bili v zadnjih 12 mesecih podvrženi zunanji varnostni reviziji?	
Človeški viri		
1.9	Ali preverjate preteklost kandidatov za zaposlitev? Prosimo, opišite postopek.	
1.10	Ali morajo vsi zaposleni, vključno z pogodbeniki in tretjimi osebami, podpisati sporazume o nerazkritju ali zaupnosti?	
1.11	Ali vsi zaposleni potrjujejo in podpisujejo, da so prebrali vašo politiko informacijske varnosti?	
1.12	Ali vsi zaposleni potrjujejo in podpisujejo, da so prebrali vašo pravilnik varovanja osebnih podatkov?	



1.13	Ali vsi novi zaposleni in pogodbeniki v vaši organizaciji prejmejo usposabljanje za ozaveščanje o informacijski varnosti in varstvu podatkov?	
1.14	Ali obstaja politika usposabljanja, ki od vseh oseb zahteva, da se vsaj enkrat letno udeležijo srečanj za ozaveščanje o informacijski varnosti/varstvu osebnih podatkov?	
1.15	Ali so vzpostavljeni disciplinski ukrepi za obravnavo kakršne koli namerne zlorabe informacij s strani zaposlenih in izvajalcev?	
Fizična varnost		
1.16	Ali obdelujete ali shranjujete podatke na lokacije družbe?	
1.17	Prosimo, navedite geografsko območje lokacij.	
1.18	Prosimo, opišite fizične varnostne ukrepe, ki varujejo objekt na tej lokaciji (npr. varnostniki, video nadzor, dostop z varnostnimi karticami)	
1.19	Ali je fizični dostop do omejenih območij odvisen od vloge posameznika?	
1.20	Ali je videonadzor nameščen na vseh fizičnih vstopnih točkah?	
1.21	Ali hranite dnevnik za vse fizične vstopne točke? Če je tako, navedite čas hrambe.	



1.22	Ali so vzpostavljeni fizični nadzorni mehanizmi za ločevanje javnega dostopa, območij za dostavo in nakladanje od drugih delov objekta?	
1.23	Prosimo, podrobno opišite postopek za obiskovalce na vaših lokacijah, npr. Ali izdajate izkaznice? Ali hranite dnevnik obiskovalcev?	
1.24	Opišite okoljske nadzorne ukrepe, ki so vzpostavljeni v objektu (npr. gašenje požara, klimatizacija itd.)	
1.25	Ali vaše podjetje obdeluje ali shranjuje podatke naše organizacije?	
Nadzor dostopa		
1.26	Ali ima vaša organizacija dokumentiran pravilnik o dostopu IT uporabnikov?	
1.27	Ali se politika sklicuje na procese za nadzor in upravljanje uporabniških računov pri: a) začetek zaposlitve b) dokončanje zaposlitve c) sprememba vloge	
1.28	Ali imate vzpostavljene kontrole za upravljanje računov privilegiranih uporabnikov? Prosimo, navedite podrobnosti.	



1.29	Katere procese in sisteme imate za spremljanje in upravljanje dostopa uporabnikov? Prosimo, navedite podrobnosti.	
1.30	Kako pogosto pregledujete dostop uporabnikov, da zagotovite, da gre za minimalni dostop, potreben za opravljanje njihovega trenutnega dela?	
1.31	Ali imate sistemsko uveljavljeno politiko gesel? Navedite vse podrobnosti o dolžini gesel, shranjenih geslih, trajanju zaklepanja itd.	
1.32	Ali vaše storitve vključujejo dostop do naših sistemov?	
Upravljanje ranljivosti		
1.33	Ali imate politiko upravljanja ranljivosti?	
1.34	Ali imate vzpostavljene postopke za zaščito vaših informacijskih storitev/sistemov pred ranljivostmi?	
1.35	Ali kot del svojih dejavnosti upravljanja ranljivosti izvajate varno konfiguracijo vseh požarnih zidov, omrežij, strežnikov, shranjevalnih naprav in uporabniških naprav? Prosimo, da navedete pregled tega postopka s podrobnostmi o vseh uporabljenih industrijskih merilih ali standardih.	



1.36	Ali imate na vseh uporabniških napravah in strežnikih omogočeno/nameščeno programsko opremo proti zlonamerni programski opremi? Kako pogosto se to posodablja?	
1.37	Kako pogosto izvajate skeniranje ranljivosti v svojih notranjih in zunanjih sistemih? Npr. tedensko, mesečno, četrtno itd. Navedite podrobnosti o skeniranjih.	
1.38	Prosim, navedite podrobnosti o vašem postopku nameščanja popravkov. Kako testirate, uvajate, upravljate in pregledujete posodobitve?	
1.39	Ali je višje vodstvo v vaši organizaciji v celoti seznanjeno z nerešenimi ranljivostmi, ki lahko neposredno vplivajo na storitev vzdrževanja?	
Upravljanje dobaviteljev		
1.40	Ali uporabljate kakšne podizvajalce, ki vam pomagajo pri zagotavljanju storitev vzdrževanja?	
1.41	Ali vodite popis vseh podizvajalcev?	
1.42	Ali podizvajalci, ki jih uporablja vaša organizacija, uporabljajo kakšne druge organizacije za opravljanje nadaljnjih storitev v	



	njihovem imenu? Če je tako, ali so ti izvajalci vključeni v popis?	
1.43	Ali imate vzpostavljen postopek za obveščanje o vseh podizvajalcih, ki jih uporabljate pri zagotavljanju storitev?	
1.44	Ali zagotavljate, da varnostni nadzor, ki ga izvaja vaša organizacija, ni zmanjšan zaradi uvedbe izdelkov ali storitev podizvajalcev?	
1.45	Ali vaši sporazumi in pogodbe s podizvajalci vključujejo varnostne in regulativne zahteve?	
1.46	Ali vsaj enkrat letno izvajate preglede informacijske varnosti s podizvajalci?	
Odziv na incidente		
1.47	Ali ima vaša organizacija načrte in postopke za upravljanje incidentov?	
1.48	Kako beležite in poročate o incidentih informacijske varnosti v vaši organizaciji? Prosimo, navedite podrobnosti.	
1.49	Kako pogosto preizkušate svoj načrt za odzivanje na incidente? Navedite datum zadnjega preizkušanja.	



1.50	Kako zagotavljate, da podizvajalci upoštevajo vaše postopke upravljanja incidentov? Prosimo, navedite podrobnosti.	
1.51	Ali storitev, ki jo nudite, zahteva interakcijo z informacijskimi sistemi? Če je tako, navedite vse podrobnosti.	
1.52	Kako hitro ste zavezani obvestiti naročnika v primeru incidenta?	
1.53	Ali izvajate teste načrta za neprekinjeno poslovanje (BCP/DRP)?	
1.54	Kdaj ste nazadnje izvajali simulacijo varnostnega incidenta?	
1.55	Ali je bilo v zadnjih 24 mesecih kakšnih kibernetских incidentov?	
Varnost oblačnih storitev		
1.56	Če zagotavljate ali boste zagotavljali storitev v oblaku, navedite vrsto modela storitve v oblaku. Ali gre za SaaS, PaaS ali IaaS?	
1.57	Ali uporabljate šifriranje za zaščito podatkov znotraj ustreznega modela storitve v oblaku? npr. podatki med prenosom, podatki v mirovanju. Navedite podrobnosti.	
1.58	Prosimo, navedite podrobne informacije o tem, kako se	



	upravljajo in shranjujejo šifrirni ključi za storitev.	
1.59	Kakšne vrste kontrol za preverjanje pristnosti/identitete uporabnikov so vzpostavljene za storitev? Ali storitev podpira enotno prijavo (SSO) ali večfaktorsko overjanje (MFA)? Prosimo, navedite podrobnosti.	
1.60	Ali storitev zagotavlja popolno zgodovino revizije in beleženje za vse administratorje in uporabnike?	
1.61	Prosimo, navedite podrobnosti o tem, kako ločujete ali boste ločili podatke od drugih strank v oblaku. Ali so vzpostavljeni ukrepi za fizično ali logično ločevanje podatkov?	
1.62	Ali ta storitev gostuje v vašem lastnem podatkovnem centru? Če ne, navedite podatke o tretji osebi, ki gosti storitev.	
1.63	Navedite vse lokacije podatkovnih centrov, ki shranjujejo ali bodo shranjevali podatke (vključno s tistimi lokacijami, ki se uporabljajo za namene neprekinjenega poslovanja).	



1.64	Ali kot del storitve izvajate varnostne kopije podatkov? Če je tako, podrobno opišite obdobja hrambe varnostnih kopij in lokacijo(-e) podatkovnih centrov, kjer se varnostne kopije podatkov nahajajo.	
1.65	Ali uporabljate požarne zidove za zaščito podatkov pred nezaupanja vrednimi omrežji? Navedite, ali gre za požarne zidove aplikacij in/ali omrežja.	
1.66	Ali se uporabljajo sistemi za odkrivanje/preprečevanje vdorov?	
1.67	Ali je platforma vsako leto predmet neodvisnega penetracijskega testa tretje osebe? Navedite datum zadnjega testa.	
1.68	Kako pogosto se izvajajo penetracijski testi storitve?	
1.69	Navedite datum zadnjega penetracijskega testa storitve in ime organizacije, ki je izvedla test.	
1.70	Če so bile pri zadnjem preizkusu storitve ugotovljene kritične, visoke ali srednje ugotovitve, ali so bile te zdaj odpravljene? Če ne, kdaj pričakujete, da bo to končano?	



1.71	Kako zagotavljate, da bodo podatki zaščiteni pred kibernetiskim napadom, npr. zavrnitvijo storitve, ki je lahko usmerjen na eno od vaših drugih strank v oblaku? Navedite podrobnosti.	
1.72	Kako izvajate varno odstranjevanje podatkov stran, ko niso več potrebni? Prosim, podrobno opišite postopek.	
Varnost programske opreme/sistema		
1.73	Ali kot del storitve zagotavljate ali dobavljate programsko opremo?	
1.74	Ali izvajate razvoj programske opreme? Če je tako, ali uporabljate določeno metodologijo razvoja programske opreme? Prosim, sporočite, če to storitev izvaja tretja oseba.	
1.75	Kako zagotovite, da vaši razvijalci programske opreme ali tretje osebe uporabljajo varna načela kodiranja?	
1.76	Ali načela varnega kodiranja upoštevajo modeliranje groženj pri načrtovanju kontrol na ravni aplikacije (npr. validacija vnosa podatkov itd.) za ublažitev ugotovljenih tveganj?	
1.77	Ali je razvita/dobavljena programska oprema predmet neodvisnega varnostnega	



	pregleda? Navedite podrobnosti o postopku pregleda, vključno s pogostostjo pregledov in datumom zadnjega pregleda.	
1.78	Ali dokumentacija programske opreme pojasnjuje, kako jo varno namestiti, konfigurirati in/ali uporabljati, in ali postopek uvajanja sledi tem navodilom?	
1.79	Ali dokumentacija programske opreme pojasnjuje, kako okrepiti osnovno infrastrukturo in ali postopek uvajanja sledi tem navodilom?	
1.80	Prosim, opišite postopek za odpravljanje ranljivosti programske opreme.	
1.81	Kako svojim strankam/kupcem posredujete informacije o znanih ranljivostih programske opreme?	
1.82	Ali se spremembe programske opreme testirajo, pregledujejo in uporabljajo z uporabo dokumentiranega postopka upravljanja sprememb? Prosim, opišite.	
Umetna inteligenca		
1.83	Ali uporabljate kakršne koli izdelke umetne inteligence (UI) kot del storitve, ki jo zagotavljate?	



1.84	Če kot del storitve uporabljate kakršne koli izdelke umetne inteligence, navedite vse podrobnosti.	
------	--	--

Kraj in datum:

Podjetje:

Podpis in žig odgovorne osebe: