Na osnovu člana 7. stav 4. Zakona o informacionoj bezbednosti („Službeni glasnik RS”, broj 6/16) i člana 42. stav 1. Zakona o Vladi („Službeni glasnik RS”, br. 55/05, 71/05 – ispravka, 101/07, 65/08, 16/11, 68/12 – US, 72/12, 7/14 – US i 44/14),

Vlada donosi

UREDBU
o bližem uređenju mera zaštite informaciono-komunikacionih sistema od posebnog značaja

Predmet Uredbe

Član 1.

Ovom uredbom bliže se uređuju mere zaštite informaciono-komunikacionih sistema od posebnog značaja (u daljem tekstu: mere zaštite).

Uspostavljanje organizacione strukture, sa utvrđenim poslovima i odgovornostima zaposlenih, kojom se ostvaruje upravljanje informacionom bezbednošću u okviru operatora IKT sistema od posebnog značaja

Član 2.

Operator IKT sistema od posebnog značaja (u daljem tekstu: operator IKT sistema) je dužan da, u okviru organizacione strukture, u skladu sa prirodom, obimom i složenošću poslovanja utvrdi poslove i odgovornosti zaposlenih u cilju upravljanja informacionom bezbednošću.

Operator IKT sistema utvrđuje, u okviru organizacione strukture, poslove i odgovornosti zaposlenih za zaštitu informacionih dobara, odnosno sredstava i imovine za nadzor nad poslovnim procesima od značaja za informacionu bezbednost, za upravljanje rizicima u oblasti informacione bezbednosti, kao i za poslove predviđene procedurama u oblasti informacione bezbednosti.

Podela odgovornosti zaposlenih treba da se izvrši tako da se onemogući neovlašćena ili nenamerna izmena, oštećenje ili zloupotreba sredstava, odnosno informacionih dobara operatora IKT sistema, kao i da se onemogući pristup, izmena ili korišćenje sredstava bez ovlašćenja i bez evidencije o tome.

Operator IKT sistema uspostavlja procedure radi praćenja aktivnosti, revizije i nadzora u okviru upravljanja informacionom bezbednošću.

Prilikom utvrđivanja odgovornosti zaposlenih potrebno je predvideti i odgovornost za obaveštavanje nadležnih organa o incidentima u IKT sistemu, u skladu sa propisima.

Operator IKT sistema utvrđuje procedure komunikacije sa drugim institucijama u slučaju incidenta u cilju blagovremene prijave, odnosno rešavanja nastalog bezbedonosnog incidenta.

Postizanje bezbednosti rada na daljinu i upotrebe mobilnih uređaja

Član 3.

Operator IKT sistema koji u svom sistemu dozvoljava rad na daljinu i upotrebu mobilnih uređaja dužan je da uspostavi i održava bezbednost rada na daljinu i upotrebe mobilnih uređaja, uzimajući u obzir rizike koji mogu postojati usled neadekvatnog korišćenja mobilnih uređaja.

Operator IKT sistema je dužan da definiše uslove i ograničenja za rad na daljinu tako da se ne ugrozi bezbednost IKT sistema, pri čemu operator IKT sistema uzima u obzir fizičku bezbednost mesta i okruženja sa koga se obavlja rad na daljinu, uslove za bezbednost komunikacije između IKT sistema operatora i mesta sa kojeg se radi na daljinu, prevenciju ili svođenje na neophodni minimum obrade i čuvanja informacija na ličnom uređaju lica koje radi na daljinu, prevenciju od neovlašćenog pristupa, uslove za korišćenje lokalne mreže i bežičnih mrežnih servisa, zahteve za zaštitu od zlonamernih softvera i druge mere koje su potrebne za bezbednost rada na daljinu.

Prilikom korišćenja mobilnih uređaja mora da se obezbedi zaštita podataka od interesa za operatora IKT sistema i smanje rizici korišćenja mobilnih uređaja u nezaštićenim okruženjima (javnim mestima, mrežama sa nepoznatom ili nedovoljnom zaštitom i slično), pri čemu operator IKT sistema uzima u obzir sledeće:

1) evidenciju mobilnih uređaja;

2) mere fizičke zaštite mobilnih uređaja (od uništenja, oštećenja, gubitka ili neovlašćenog pristupa uređajima i podacima od interesa za operatora IKT sistema);

3) ograničenja za instalaciju i ažuriranje softvera;

4) instalaciju adekvatnih softvera za mobilne uređaje i njihovo redovno ažuriranje;

5) ograničenje korišćenja usluga informacionog društva koje bi ugrozile informacionu bezbednost IKT sistema;

6) kontrole pristupa mobilnom uređaju i podacima na njemu;

7) kriptografske tehnike;

8) zaštitu od virusa i drugih zlonamernih softvera;

9) daljinsko upravljanje mobilnim uređajem u slučaju incidenta, od strane ovlašćenog lica operatora IKT sistema, putem kojeg je moguće da se izvrši nepovratno brisanje podataka i onemogućavanje daljeg korišćenja uređaja;

10) uspostavljanje i održavanje rezervne kopije (backup) podataka;

11) omogućavanje bezbednog korišćenja internet servisa i aplikacija.

Ako operator IKT sistema dozvoljava u svom sistemu korišćenje privatnih mobilnih uređaja dužan je da obezbedi uslove iz stava 3. ovog člana i preduzme mere radi razdvajanja privatnog od poslovnog korišćenja ovih uređaja.

Obezbeđivanje da lica koja koriste IKT sistem odnosno upravljaju IKT sistemom budu osposobljena za posao koji rade i razumeju svoju odgovornost

Član 4.

Lica koja upravljaju IKT sistemom odnosno zaposlena lica koja koriste IKT sistem moraju da imaju adekvatan nivo obrazovanja i sposobnosti, svest o značaju poslova koje obavljaju i njihove odgovornosti koja se utvrđuje ugovorom i drugim aktima.

Kako bi lica koja koriste IKT sistem odnosno upravljaju IKT sistemom razumeli svoje odgovornosti, operator IKT sistema obučava zaposlene o važnosti informacione bezbednosti IKT sistema, merama i procedurama za zaštitu IKT sistema i njihovim obavezama.

Operator IKT sistema je dužan da pokrene odgovarajući postupak protiv lica odgovornih za narušavanje bezbednosti informacionog sistema.

Zaštita od rizika koji nastaju pri promenama poslova ili prestanka radnog angažovanja lica zaposlenih kod operatora IKT Sistema

Član 5.

Operator IKT sistema je dužan da ugovorom ili drugim aktom obaveže zaposlena i po drugim osnovama angažovana lica da nakon prestanka ili promene radnog angažovanja ne otkriva poverljive i druge informacije koje su od značaja za informacionu bezbednost IKT sistema. Dužnosti i obaveze koje ostaju važeće i posle prestanka angažovanja treba da budu sadržane u uslovima ugovora sa zaposlenim odnosno po drugom osnovu angažovanim licem.

Identifikovanje informacionih dobara i određivanje odgovornosti za njihovu zaštitu

Član 6.

Operator IKT sistema je dužan da identifikuje i klasifikuje informaciona dobra, odnosno sredstva i imovinu, putem kojih se vrši izrada, obrada, čuvanje, prenos, brisanje i uništavanje podataka u IKT sistemu, izvrši popis informacionih dobara, odnosno sredstava i imovine, i uspostavi, održava i redovno ažurira njihovu evidenciju.

Operator IKT sistema je dužan da klasifikaciju iz stava 1. ovog člana vrši prema stepenu osetljivosti i kritičnosti, uzimajući u obzir moguće posledice narušavanja poverljivosti, integriteta i raspoloživosti dobara, da dosledno primenjuje tu klasifikaciju, kao i da, u skladu s tim, obezbedi adekvatan nivo zaštite ovih dobara.

Za svako informaciono dobro, odnosno sredstvo i imovinu, potrebno je odrediti zaduženo lice za njihovu zaštitu.

Klasifikovanje podataka tako da nivo njihove zaštite odgovara značaju podataka u skladu sa načelom upravljanja rizikom iz Zakona o informacionoj bezbednosti

Član 7.

Operator IKT sistema određuje šemu klasifikacije podataka prema kojoj se podaci klasifikuju uzimajući u obzir osetljivost, važnost podataka, štetu koja može da nastane usled neovlašćenog otkrivanja, izmene ili brisanje podataka i propise koji uređuju pitanja zaštite podataka (o tajnim podacima, poslovnoj tajni, podacima o ličnosti i sl.).

Operator IKT sistema u obavezi je da definiše odgovarajući skup procedura za postupanje, obradu, skladištenje i prenošenje podataka u skladu sa šemom klasifikacije podataka iz stava 1. ovog člana.

Mere zaštite podataka koji su, u skladu sa zakonom koji uređuje oblast tajnosti podataka, označeni kao tajni, određuju se u skladu sa propisima koji regulišu ovu oblast.

Izbor i nivo primene mera zaštite podataka se zasniva na proceni rizika, potrebi za prevencijom rizika i otklanjanju posledica rizika koji se ostvario, uključujući sve vrste vanrednih okolnosti.

Zaštita nosača podataka

Član 8.

Operator IKT sistema dužan je da obezbedi sprečavanje neovlašćenog razotkrivanja, modifikovanja, uklanjanja ili uništenja informacija i sadržaja koji se čuvaju na nosačima podataka, tako što utvrđuje i primenjuje procedure za upravljanje nosačima podataka u skladu sa klasifikacijom iz člana 7. ove uredbe.

Prilikom definisanja procedura i postupanja sa nosačima podataka, treba predvideti nepovratno brisanje podataka, u slučaju kada su istekli rokovi za njihovo čuvanje i kada oni više nisu potrebni, postupak odobravanja iznošenja nosača podataka iz prostorija operatora IKT sistema, čuvanje nosača podataka na bezbednom mestu, korišćenje kriptografskih tehnika za zaštitu podataka kada je to predviđeno propisima, odnosno u drugim slučajevima kada je takva vrsta zaštite potrebna, obezbeđivanje sigurnog prenosa podataka na novi nosač podataka, čuvanje rezervnih kopija na odvojenim nosačima podataka i druge mere i postupke za zaštitu nosača podataka.

Operator IKT sistema treba da predvidi procedure za bezbedno rashodovanje i uništavanje nosača podataka kada više nisu potrebni, a koje treba da na minimum svedu rizik od pristupa podacima od strane neovlašćenih lica.

Nosači podataka treba da budu zaštićeni od neovlašćenog pristupa, zloupotrebe ili oštećenja prilikom transporta, obezbeđivanjem pouzdanog transporta i pouzdanih osoba koje prenose nosače podataka i obezbeđivanjem adekvatne ambalaže u cilju fizičke zaštite prilikom transporta.

Operator IKT sistema određuje za koje podatke, u skladu sa šemom klasifikacije podataka, treba voditi evidenciju o korišćenju nosača podataka i preduzetim postupcima u vezi sa zaštitom podataka i nosača podataka.

Ograničenje pristupa podacima i sredstvima za obradu podataka

Član 9.

Ograničenje pristupa podacima i sredstvima za obradu podataka podrazumeva definisanje preciznih pravila pristupa, tako što se definiše ko ima pravo čemu da pristupi i koja su ograničenja pristupa podacima i sredstvima za obradu podataka, a vodeći računa o specifičnostima podataka i opreme i odgovornostima i radnim zaduženjima lica koja pristupaju podacima i opremi.

Ograničenje pristupa podrazumeva hardversko, odnosno softversko ograničenje pristupa podacima i sredstvima za obradu podataka, uključujući i fizičko ograničenje pristupa podacima i sredstvima.

Ograničenje pristupa vrši se u skladu sa klasifikacijom podataka iz člana 7. ove uredbe.

Operator IKT sistema treba da obezbedi pristup mreži i mrežnim uslugama samo licima koja imaju ovlašćenja za korišćenje.

Odobravanje ovlašćenog pristupa i sprečavanje neovlašćenog pristupa IKT sistemu i uslugama koje IKT sistem pruža

Član 10.

Operator IKT sistema je u obavezi da predvidi proceduru za odobravanje i ukidanje ovlašćenog pristupa IKT sistemu i uslugama koje IKT sistem pruža, tako što predviđa uslove za odobravanje i ukidanje ovlašćenog pristupa, proveru adekvatnosti odobrenog nivoa pristupa i dodelu jedinstvene identifikacione oznake licu kojem se odobrava pristup.

Operator IKT sistema vodi evidenciju o dodeljenim i oduzetim oznakama, utvrđuje uslove za korišćenje zajedničke identifikacione oznake u slučajevima kada je to neophodno, definiše način i uslove onemogućavanja i uklanjanja jedinstvenih identifikacionih oznaka, kao i uslove za dodelu i korišćenje administratorskih prava.

Licima kojima se odobrava ovlašćeni pristup omogućuje se pristup na osnovu podataka za autentikaciju (lozinke, kriptografski ključevi, podaci skladišteni na tokenima i sl.).

Dodela i korišćenje administratorskih prava pristupa treba da bude ograničena i kontrolisana.

Operator IKT sistema dužan je da obezbedi mehanizam za ukidanje prava pristupa u slučajevima promene radnog mesta, prestanka radnog odnosa i, po potrebi, u drugim slučajevima.

Utvrđivanje odgovornosti korisnika za zaštitu sopstvenih sredstava za autentikaciju

Član 11.

Operator IKT sistema propisuje način autentikacije lica kome je odobren pristup sistemu, odnosno korisnika.

Lice kome se odobrava ovlašćeni pristup, odnosno korisnik, mora da se obaveže da neće otkrivati svoje podatke za autentikaciju.

Operator IKT sistema predviđa načine kreiranja i čuvanja podataka za autentikaciju koji obezbeđuju visok nivo bezbednosti i zaštite od otkrivanja od strane drugih lica.

Operator IKT sistema predviđa obavezu promene podataka za autentikaciju u slučaju da su podaci otkriveni, ili je povećana opasnost od njihovog otkrivanja.

Predviđanje odgovarajuće upotrebe kriptozaštite radi zaštite tajnosti, autentičnosti odnosno integriteta podataka

Član 12.

Radi zaštite tajnosti, autentičnosti i integriteta podataka, operator IKT sistema treba da razmotri korišćenje odgovarajućih mera kriptozaštite, uzimajući u obzir osetljivost informacija koje treba da se štite, poslovne procese koji se sprovode, nivo zahtevane zaštite, implementaciju primenjenih kriptografskih tehnika i upravljanje kriptografskim ključevima.

Upravljanje kriptografskim ključevima obuhvata njihov celokupan životni ciklus, uključujući generisanje, skladištenje, arhiviranje, preuzimanje, raspodelu, povlačenje i uništavanje ključeva.

Operator IKT sistema treba da posebno vodi računa o zaštiti sredstava kriptozaštite od svih oblika kompromitacije.

Fizička zaštita objekata, prostora, prostorija odnosno zona u kojima se nalaze sredstva i dokumenti IKT sistema i obrađuju podaci u IKT sistemu

Član 13.

Operator IKT sistema dužan je da spreči neovlašćen fizički pristup objektima, prostorima, prostorijama odnosno bezbednosnim zonama u kojima se nalaze sredstva i dokumenti IKT sistema i obrađuju podaci u IKT sistemu.

U slučaju kada posebnim propisima nije predviđena obaveza uspostavljanja bezbednosnih zona, operator IKT sistema može da predvidi mere fizičko-tehničke zaštite prostorija u kojima se nalaze sredstva i dokumenti IKT sistema i obrađuju podaci u IKT sistemu, kao što su ugradnja alarmnih uređaja, kontrola ulaska uz obavezno nošenje vidljive identifikacije za sve vreme boravka i druge kojima se obezbeđuje fizičko-tehnička zaštita.

Operator IKT sistema dužan je da predvidi i primeni mere fizičke zaštite u slučaju elementarnih nepogoda, zlonamernih napada, nesreća ili namernog uništavanja objekata, prostorija, sredstava i dokumenata IKT sistema.

Zaštita od gubitka, oštećenja, krađe ili drugog oblika ugrožavanja bezbednosti sredstava koja čine IKT system

Član 14.

Operator IKT sistema dužan je da zaštiti sredstva koja čine IKT sistem od gubitka, oštećenja, krađe ili drugog oblika ugrožavanja bezbednosti.

U cilju zaštite sredstava, operator IKT sistema mora da vodi računa o postavljanju sredstava na bezbedna mesta, eliminiše nepotreban pristup u prostor u kome se nalaze, vrši redovne provere zaštićenosti sredstava od krađa, požara, elektromagnetnih zračenja i drugih pretnji i prati uslove okoline (temperaturu, vlažnost i dr.) koji bi mogli negativno da utiču na rad sredstava.

Sredstva treba da budu zaštićena u slučaju poremećaja u distribuciji električne energije, telekomunikacionih kapaciteta, vode, gasa, ventilacije obezbeđivanjem alternativnih rešenja koja omogućuju nastavak rada IKT sistema.

Izmeštanje imovine IKT sistema može da se vrši samo uz prethodno odobrenje ovlašćenog lica, uz primenu bezbednosnih mehanizama, uzimajući u obzir različite rizike prilikom rada izvan prostorija organizacije.

Obezbeđivanje ispravnog i bezbednog funkcionisanja sredstava za obradu podataka

Član 15.

U cilju obezbeđivanja ispravnog i bezbednog funkcionisanja sredstava za obradu podataka, operator IKT sistema definiše procedure za rukovanje sredstvima, koje se odnose na otpočinjanje i završetak pristupa informacionom sistemu, pravljenje rezervnih kopija, održavanje opreme, rukovanje nosačima podataka, kontrolu pristupa u prostorije sa serverskom infrastrukturom, komunikacionom opremom i sistemima za skladištenje podataka, kao i u slučajevima izmeštanja delova IKT sistema.

Operator IKT sistema uspostavlja procedure za postupanje u slučaju promena u organizaciji, poslovnim procesima, sredstvima za obradu informacija i na sistemima koje imaju uticaj na bezbednost informacija i predviđa odgovornosti za sprovođenje definisanih procedura.

Operator IKT sistema kontinuirano nadzire i proverava funkcionisanje sredstava za obradu podataka i predviđa buduće promene koje mogu uticati na bezbednost IKT sistema i, u skladu sa tim, planira odgovarajuće mere.

Operator IKT sistema mora međusobno razdvojiti okruženja za razvoj, testiranje i operativan rad da bi se smanjili rizici od neovlašćenog pristupa ili promena u radnom okruženju.

Zaštita podataka i sredstva za obradu podataka od zlonamernog softvera

Član 16.

Zaštita podataka i sredstava za obradu podataka treba da obuhvati mere za otkrivanje zlonamernog softvera i za otklanjanje štete od zlonamernog softvera, uključujući odgovarajuće kontrole pristupa sistemu, sprečavanje unošenja i izvršavanja zlonamernih softvera, sprečavanje pristupanja rizičnim veb sajtovima, kontinuirano ažuriranje softvera za otkrivanje zlonamernih softvera, upravljanje ranjivostima i proverama IKT sistema, implementaciju procedura kao i podizanje svesti o rizicima od posledica delovanja zlonamernog softvera.

Zaštita od gubitka podataka

Član 17.

Zaštita od gubitka podataka postiže se redovnom izradom rezervnih kopija podataka, softvera i sistema putem odgovarajućih sredstava za izradu rezervnih kopija.

Operator IKT sistema definiše vreme čuvanja i zaštite rezervnih kopija, obim i učestalost rezervnih kopija, bezbedno mesto čuvanja rezervnih kopija, obezbeđuje fizičku zaštitu rezervnih kopija i zaštitu od spoljašnjih uticaja, proverava nosače podataka kako bi se osiguralo njihovo ispravno funkcionisanje i pouzdanost u skladu sa planom izrade rezervnih kopija.

Operator IKT sistema vrši izradu rezervnih kopija koje treba da obuhvate sve sistemske informacije, aplikacije i podatke koji su neophodni za oporavak celokupnog sistema u slučaju nastupanja posledica izazvanih vanrednim okolnostima.

Čuvanje podataka o događajima koji mogu biti od značaja za bezbednost IKT Sistema

Član 18.

Operator IKT sistema treba da obezbedi da se u IKT sistemu formiraju zapisi o događajima (logovi) u vezi aktivnosti korisnika, greškama i događajima u vezi sa informacionom bezbednošću, a koji se moraju čuvati i redovno proveravati.

Sredstva za zapisivanje i zapisi treba da budu zaštićeni od neovlašćenog pristupa i promene.

U okviru IKT sistema zapisuju se aktivnosti administratora i korisnika i redovno preispituju u cilju zaštite.

U cilju obezbeđivanja pouzdanosti zapisa, vremena u svim podsistemima IKT sistema moraju biti sinhronizovana međusobno, kao i sa referentnim tačnim vremenom.

Obezbeđivanje integriteta softvera i operativnih Sistema

Član 19.

Operator IKT sistema predviđa i sprovodi procedure kojima se obezbeđuje kontrola integriteta instaliranog softvera i operativnih sistema, ažuriranje softvera i operativnih sistema od strane ovlašćenog administratora, odnosno ovlašćenog lica, primena sistema za kontrolu konfiguracije softvera, uspostavljanje mogućnosti povratka na prethodno stanje pre implementacije promena u sistemu, čuvanje prethodnih verzija softvera u slučaju neočekivanih situacija i druge mere u cilju smanjenja rizika od oštećenja softvera i operativnih sistema.

Zaštita od zloupotrebe bezbednosnih slabosti IKT Sistema

Član 20.

U cilju zaštite IKT sistema od zloupotrebe bezbednosnih slabosti, operator IKT sistema vrši analizu IKT sistema i utvrđuje stepen izloženosti IKT sistema potencijalnim bezbednosnim slabostima, i, u skladu sa tim, preduzima odgovarajuće mere koje se odnose na uklanjanje prepoznatih slabosti ili primenu drugih vrsta zaštite IKT sistema.

Operator IKT sistema onemogućava neodobreno instaliranje softvera na uređajima koji mogu dovesti do izloženosti IKT sistema bezbednosnim slabostima.

Obezbeđivanje da aktivnosti na reviziji IKT sistema imaju što manji uticaj na funkcionisanje Sistema

Član 21.

Prilikom sprovođenja revizije IKT sistema, operator IKT sistema mora da obezbedi da revizija ima što manji uticaj na funkcionisanje sistema, tako što planira adekvatno vreme sprovođenja revizije i redosled aktivnosti koji ne ometaju poslovne procese operatora IKT sistema.

Zaštita podataka u komunikacionim mrežama uključujući uređaje i vodove

Član 22.

U cilju zaštite podataka u komunikacionim mrežama, uređajima i vodovima vrši se njihova kontrola i zaštita od neovlašćenog pristupa, pri čemu se predviđa uspostavljanje procedura i odgovornosti za upravljanje mrežnom opremom, odgovornost za rad mreže, posebne kontrole za zaštitu poverljivosti i integriteta podataka koji prolaze putem javnih ili bežičnih mreža.

Operator IKT sistema redovno proverava da li postoji adekvatna bezbednost mrežnih servisa.

Operator IKT sistema, u cilju posebne zaštite pojedinih IKT servisa, može izvršiti segmentiranje mreže u cilju izolacije ovih servisa i ograničiti pristup samo ovlašćenim licima.

Kablovi za napajanje i komunikacioni kablovi koji prenose podatke ili koji predstavljaju podršku informacionim uslugama treba da budu zaštićeni od prisluškivanja, krađe, ometanja ili oštećenja.

Bezbednost podataka koji se prenose unutar operatora IKT sistema, kao i između operatora IKT sistema i lica van operatora IKT Sistema

Član 23.

Zaštita podataka koji se prenose komunikacionim sredstvima unutar operatora IKT sistema, između operatora IKT sistema i lica van operatora IKT sistema, obezbeđuje se uspostavljanjem procedura i adekvatnih kontrola.

Procedurama se predviđa zaštita od prisluškivanja, modifikovanja, pogrešnog usmeravanja i uništenja podataka, otkrivanje i zaštita od zlonamernog softvera, eventualno korišćenje kriptografskih tehnika i druge adekvatne mere.

Kada se prenos podataka vrši između operatora IKT sistema i lica van operatora IKT sistema, mogu se zaključiti sporazumi o prenosu podataka i sporazumi o poverljivosti ili neotkrivanju koji sadrže odredbe o bezbednosti prenosa podataka.

U slučaju iz stava 3. ovog člana, za prenos podataka o ličnosti potrebno je ispuniti uslove predviđene zakonom kojim se uređuje zaštita podatka o ličnosti.

Pitanja informacione bezbednosti u okviru upravljanja svim fazama životnog ciklusa IKT sistema odnosno delova sistema

Član 24.

Zahtevi za informacionu bezbednost moraju da se ispune u svim fazama životnog ciklusa IKT sistema odnosno delova sistema, što podrazumeva fazu projektovanja IKT sistema, uspostavljanja novog ili menjanje postojećeg IKT sistema, odnosno delova sistema, i nabavku proizvoda potrebnih za funkcionisanje IKT sistema.

Uspostavljanje novog IKT sistema, odnosno menjanje postojećeg, obuhvata sprovođenje procedure dokumentovanja, definisanja zahteva za informacionu bezbednost, proveru ispunjenosti zahteva, kontrolisanje i upravljanje postupka uvođenja novog, odnosno menjanja postojećeg IKT sistema.

Zahtevi za informacionu bezbednost moraju da se ispune i kada se vrši prenos informacija putem javnih komunikacionih mreža i koriste aplikativne usluge putem javnih komunikacionih mreža.

Prilikom poveravanja aktivnosti u vezi sa IKT sistemom trećim licima, potrebno je da operator IKT sistema nadgleda i prati aktivnosti razvoja IKT sistema.

Zaštita podataka koji se koriste za potrebe testiranja IKT sistema odnosno delova Sistema

Član 25.

Za potrebe testiranja IKT sistema odnosno delova sistema operator IKT sistema koristi podatke koji nisu osetljivi, koje štiti, čuva i kontroliše na odgovarajući način.

Ako se za potrebe testiranja koriste poverljive informacije, odnosno lični podaci, potrebno ih je upotrebljavati i štititi u skladu sa propisima i ovlašćenjima.

Zaštita sredstava operatora IKT sistema koja su dostupna pružaocima usluga

Član 26.

Operator IKT sistema u svojim procedurama predviđa nivo dostupnosti i vrstu informacija i sredstva kojima mogu da pristupe pružaoci usluga, načine pristupa informacijama i sredstvima i nadzor nad pristupom.

Operator IKT sistema treba da identifikuje i uspostavi procedure bezbednosti informacija koje se konkretno bave pristupom informacijama pružaoca usluga unutar organizacije.

Obaveze pružaoca usluga u vezi sa informacijama i sredstvima koja su dostupna pružaocima usluga operatora IKT sistema regulišu se sporazumom između operatora IKT sistema i pružaoca usluga, čijim odredbama se obezbeđuje adekvatan nivo zaštite informacija i sredstava, u skladu sa propisima i tehničkim standardima.

Operator IKT sistema dužan je da obezbedi da pružalac usluga obavlja poverene aktivnosti u skladu sa aktom o bezbednosti IKT sistema, odnosno drugim aktima kojima se uređuje bezbednost njegovog informacionog sistema.

Održavanje ugovorenog nivoa informacione bezbednosti i pruženih usluga u skladu sa uslovima koji su ugovoreni sa pružaocem usluga

Član 27.

U cilju održavanja ugovorenog nivoa informacione bezbednosti i pruženih usluga u skladu sa uslovima koji su ugovoreni sa pružaocem usluga, operator IKT sistema uspostavlja mehanizme nadzora nad pružanjem usluga, imenuje lice koje je zaduženo za praćenje realizacije pružanja usluga i kontrolu ispunjenosti nivoa informacione bezbednosti, primenom odgovarajućih procedura i uspostavom nadzora.

Prevencija i reagovanje na bezbednosne incidente, što podrazumeva adekvatnu razmenu informacija o bezbednosnim slabostima IKT sistema, incidentima i pretnjama

Član 28.

Operator IKT sistema u obavezi je da utvrdi procedure kojima se definišu odgovorna lica zadužena za prevenciju i reagovanje, plan postupanja u slučaju opasnosti od nastanka bezbednosnih incidenata ili nastanka bezbednosnih incidenata, obavezu vođenja evidencije o preduzetim aktivnostima, obavezu izveštavanja i razmenu informacija o bezbednosnim slabostima IKT sistema, incidentima i pretnjama.

Operator IKT sistema treba da obaveže sve zaposlene i pružaoce usluga da odgovornom licu iz stava 1. ovog člana bez odlaganja prijavljuju bezbednosne slabosti, pretnje i incidente u IKT sistemu.

Operator IKT sistema je u obavezi da odredi odgovorno lice za obaveštavanje nadležnih organa o incidentima u IKT sistemu koji mogu da imaju značajan uticaj na narušavanje informacione bezbednosti.

Operator IKT sistema treba da definiše i primenjuje procedure koje trebaju da obezbede procese za identifikaciju, prikupljanje i čuvanje informacija koje mogu da posluže kao dokaz radi pokretanja disciplinskog, prekršajnog ili krivičnog postupka.

Mere koje obezbeđuju kontinuitet obavljanja posla u vanrednim okolnostima

Član 29.

Operator IKT sistema treba da predvidi mere kojima se obezbeđuje obavljanje poslova u vanrednim okolnostima, a koje podrazumevaju održavanje informacione bezbednosti na zadovoljavajućem nivou, definisanje odgovornosti, planova, postupaka u slučaju vanrednih događaja i procedura za oporavak IKT

sistema, u okviru redovnih procedura za održavanje informacione bezbednosti ili donošenjem posebnih procedura.

Operator IKT sistema treba da uspostavi, dokumentuje, implementira i održava procese, procedure i kontrole da bi osigurao zahtevani nivo kontinuiteta poslovanja tokom vanredne situacije.

Operator IKT sistema treba da verifikuje uspostavljene i implementirane kontrole kontinuiteta poslovanja u redovnim uslovima rada, kako bi one bile važeće i efektivne tokom vanredne situacije.

Operator IKT sistema treba da identifikuje zahteve za dostupnost IKT sistema. Redundantne komponente treba razmotriti onda kada se dostupnost ne može garantovati korišćenjem postojećih arhitektura sistema.

Završna odredba

Član 30.

Ova uredba stupa na snagu osmog dana od dana objavljivanja u „Službenom glasniku Republike Srbije”.

05 broj 110-9472/2016-1
U Beogradu, 17. novembra 2016. godine
Vlada
Predsednik,
Aleksandar Vučić, s.r.