

1742.

Komisija za tržište kapitala (u daljem tekstu: Komisija) na osnovu člana 53a stav 6 Zakona o otvorenim investicionim fondovima sa javnom ponudom ("Službeni list Crne Gore", br. 023/25 od 11.03.2025, 117/25 od 15.10.2025, 014/26 od 09.02.2026)- (u daljem tekstu: Zakon), na 190. sjednici od 2. 7. 2026. godine, je donijela

PRAVILA

O DIGITALNOJ OTPORNOSTI DRUŠTAVA ZA UPRAVLJANJE OTVORENIM INVESTICIONIM FONDOVIMA SA JAVNOM PONUDOM

("Službeni list Crne Gore", br. 096/26 od 06.07.2026)

Opšte odredbe

Član 1

Ovim pravilima propisuju se način, postupak, rokovi, standardi i mjere za uspostavljanje, održavanje i nadzor digitalne operativne otpornosti društava za upravljanje otvorenim investicionim fondovima sa javnom ponudom (u daljem tekstu: društvo za upravljanje), uključujući upravljanje rizicima informacione i komunikacione tehnologije (IKT), testiranje digitalne otpornosti, postupanje u slučaju IKT incidenata i saradnju sa pružaocima IKT usluga.

Predmet

Član 2

Društvo za upravljanje dužno je da uspostavi, sprovodi i redovno održava politike, mjere i postupke kojima se obezbjeđuje digitalna operativna otpornost, zaštita mrežnih i informacionih sistema i kontinuitet poslovanja, u skladu sa ovim pravilima i zakonom.

Obaveze iz stava 1 ovog člana obuhvataju naročito:

1. upravljanje rizicima informacione i komunikacione tehnologije (IKT);
2. planiranje i sprovođenje mjera kontinuiteta poslovanja i oporavka u oblasti IKT;
3. testiranje digitalne otpornosti i sprovođenje redovnih provjera bezbjednosti;
4. upravljanje rizicima u vezi sa pružaocima IKT usluga;
5. prijavljivanje značajnih IKT incidenata Komisiji u propisanim rokovima.

Društvo za upravljanje dužno je da prilagodi politike i mjere digitalne otpornosti svojoj veličini, prirodi i složenosti poslovanja, u skladu sa načelom proporcionalnosti.

Upravljanje IKT rizicima

Član 3

Društvo za upravljanje dužno je da uspostavi i primjenjuje okvir za upravljanje rizicima informacione i komunikacione tehnologije (IKT), koji obuhvata identifikovanje, procjenu, praćenje i upravljanje svim rizicima koji mogu uticati na bezbjednost, integritet, raspoloživost ili pouzdanost mrežnih i informacionih sistema.

Okvir iz stava 1 ovog člana mora najmanje obuhvatati:

1. politike i procedure za bezbjedno korišćenje i zaštitu IKT sredstava i podataka;
2. postupke za klasifikaciju informacija i upravljanje pristupom;
3. mjere za upravljanje promjenama, otkrivenim ranjivostima i ažuriranjima sistema;
4. vođenje evidencija o IKT resursima, aplikacijama i infrastrukturnim komponentama;
5. nadzor i vođenje dnevnčkih zapisa (logova) radi otkrivanja i praćenja incidenata;
6. obavezu redovnog praćenja i procjene izloženosti rizicima, uključujući rizike sajber napada i gubitka podataka.

Društvo za upravljanje dužno je da najmanje jednom godišnje preispita politiku upravljanja IKT rizicima i usklade je sa promjenama u poslovnim procesima, tehničkim rješenjima i regulatornim zahtjevima.

Kontinuitet poslovanja i oporavak u oblasti IKT

Član 4

Društvo za upravljanje dužno je da uspostavi, sprovodi i redovno testira politike i planove kontinuiteta poslovanja i oporavka u oblasti informacione i komunikacione tehnologije (IKT), kojima se obezbjeđuje nesmetano obavljanje ključnih poslovnih funkcija u slučaju poremećaja u radu mrežnih i informacionih sistema.

Politike i planovi iz stava 1 ovog člana moraju najmanje sadržati:

1. postupke za održavanje dostupnosti i integriteta podataka i usluga u slučaju tehničkih ili bezbjednosnih incidenata;
2. definisane ciljeve oporavka (RTO - maksimalno prihvatljivo vrijeme prekida rada i RPO - maksimalno prihvatljiv gubitak podataka izražen vremenom) za svaku ključnu funkciju;
3. mjere za obezbjeđivanje alternativnih lokacija, sistema i komunikacionih kanala;
4. uloge, odgovornosti i komunikacione procedure u slučaju incidenta;
5. način dokumentovanja i arhiviranja svih aktivnosti preduzetih tokom oporavka.

Politike i planovi kontinuiteta poslovanja i oporavka moraju se testirati najmanje jednom godišnje, kroz različite scenarije rizika, uključujući prekid rada informacionih sistema, gubitak podataka i sajber napade, a o rezultatima testiranja vodi se evidencija, a utvrđene nepravilnosti i slabosti se bez odlaganja otklanjaju.

Društvo za upravljanje dužno je da obezbijedi redovno ažuriranje politika i planova iz ovog člana, u skladu sa promjenama u organizacionoj strukturi, informacionim sistemima i regulatornim zahtjevima.

Osnovna testiranja digitalne operativne otpornosti

Član 5

Društvo za upravljanje dužno je da redovno sprovodi osnovna testiranja digitalne operativne otpornosti svojih mrežnih i informacionih sistema, radi provjere sposobnosti za sprečavanje, otkrivanje i reagovanje na događaje koji mogu ugroziti bezbjednost, dostupnost, integritet i povjerljivost podataka.

Osnovna testiranja iz stava 1 ovog člana obuhvataju najmanje:

1. testove tehničke bezbjednosti, uključujući provjere ranjivosti i penetracione testove,
2. provjere funkcionalnosti planova kontinuiteta poslovanja i oporavka (BCP/DR),
3. testove integriteta i dostupnosti podataka, uključujući provjere rezervnih kopija,
4. vježbe reagovanja na incidente, uključujući simulacione ("tabletop") vježbe.

Osnovna testiranja se sprovode najmanje jednom godišnje, a obim i metodologija se prilagođavaju veličini, prirodi i složenosti poslovanja subjekta.

Ako se tokom osnovnih testiranja utvrde slabosti ili nedostaci, društvo za upravljanje dužno je da bez odlaganja preduzme korektivne mjere, koje dokumentuju i evidentiraju.

Svi rezultati sprovedenih osnovnih testiranja čuvaju se u internim evidencijama najmanje pet godina i dostavljaju Komisiji na njen zahtjev.

Upravljanje IKT rizicima trećih lica

Član 6

Društvo za upravljanje dužno je da uspostavi politike i postupke za upravljanje rizicima koji proizlaze iz korišćenja usluga IKT trećih lica, uključujući i pružaoca usluga u oblaku (cloud servise), hosting, održavanje, razvoj softvera, sajber bezbjednost i slične IKT funkcije.

Prije zaključivanja ugovora sa IKT trećim licem, društvo za upravljanje obavezno je da sprovede procjenu rizika i provjeru pouzdanosti (due diligence) pružaoca, koja obuhvata najmanje:

1. tehničke i organizacione mjere bezbjednosti;
2. sposobnost pružaoca da obezbijedi kontinuitet poslovanja i oporavak u slučaju incidenta;
3. lokaciju i način obrade podataka;
4. usklađenost sa propisima o zaštiti podataka i informacionoj bezbjednosti;
5. mogućnost raskida ugovora i migracije podataka bez ugrožavanja poslovanja.

Ugovor kojim se uređuje korišćenje IKT usluga trećih lica mora sadržati najmanje:

1. obaveze pružaoca u pogledu bezbjednosti podataka i upravljanja IKT rizikom;
2. zahtjeve za kontinuitet poslovanja i oporavak sistema;
3. obavezu prijavljivanja značajnih IKT incidenata društvu i Komisiji;
4. pravo pristupa, nadzora, inspekcije i revizije od strane društva, depozitara i Komisije;

5. ograničenja u vezi sa podugovaranjem (sub-outsourcing) i obavezu prethodnog odobrenja;

6. uslove i rokove za raskid ugovora i povrat ili brisanje podataka.

Društvo za upravljanje dužno je da vodi registar svih IKT trećih lica, koji sadrži:

1. naziv pružaoca i opis usluga,
2. klasifikaciju rizika povezanih sa uslugom,
3. datume početka i isteka ugovora,
4. plan kontinuiteta poslovanja i kontakt tačke za hitne slučajeve,
5. procjenu o eventualnom statusu pružaoca kao kritičnog IKT trećeg lica.

Kritičnim IKT trećim licem smatra se pružalac čije usluge su od suštinskog značaja za kontinuitet poslovanja društva za upravljanje, a čiji bi prestanak pružanja usluga ili ozbiljan incident mogao izazvati:

1. značajan prekid poslovanja,
2. gubitak ili kompromitaciju podataka članova fonda,
3. narušavanje integriteta finansijskih podataka ili tržišnih informacija,
4. nemogućnost ispunjavanja regulatornih obaveza.

Pri ocjeni da li se pružalac smatra kritičnim, društvo uzima u obzir:

1. obim, složenost i trajanje usluge,
2. stepen zavisnosti poslovnih funkcija od te usluge,
3. mogućnost zamjene pružaoca u razumnom roku,
4. procijenjeni uticaj na članove fonda i finansijsku stabilnost,
5. učestalost i istorijat bezbjednosnih incidenata tog pružaoca.

Društvo za upravljanje obavezno je da redovno, a najmanje jednom godišnje, preispita status svih IKT trećih lica, ažurira registar i procjenu rizika, te preduzme mjere za smanjenje zavisnosti od jednog ili malog broja pružalaca usluga.

Prijavljivanje IKT incidenata

Član 7

Društvo za upravljanje dužno je da bez odlaganja, a najkasnije u roku od 24 sata od saznanja, obavijesti Komisiju o svakom značajnom IKT incidentu koji ima ili može imati negativan uticaj na kontinuitet poslovanja, bezbjednost podataka članova fonda, mrežne i informacione sisteme ili pružanje usluga društva za upravljanje.

Značajnim IKT incidentom, u smislu ovih pravila, smatra se događaj koji je doveo ili bi mogao dovesti do:

1. prekida u radu ključnih sistema dužeg od 30 minuta;
2. neovlašćenog pristupa, gubitka, izmjene ili objavljivanja povjerljivih podataka;
3. narušavanja integriteta finansijskih podataka ili podataka o članovima UCITS fonda;
4. nemogućnosti obrade transakcija ili pristupa korisničkim uslugama;
5. potrebe aktiviranja planova kontinuiteta poslovanja ili oporavka sistema;
6. ozbiljnog narušavanja reputacije društva za upravljanje.

Obavještenje iz stava 1 sadrži najmanje:

1. osnovne podatke o prijavi (naziv subjekta, datum i vrijeme otkrivanja incidenta, kontakt osobu),
2. kratak opis incidenta i pogođenih sistema,
3. procjenu uticaja na poslovanje,
4. preduzete i planirane mjere sanacije,
5. preliminaru procjenu uzroka i rizika od ponavljanja.

Nakon početnog obavještenja, društvo za upravljanje dostavlja završni izvještaj Komisiji u roku od 10 radnih dana, koji sadrži detaljnu analizu uzroka, obim uticaja, mjere sanacije i preporuke za sprječavanje ponavljanja.

U slučaju posebno ozbiljnih IKT incidenata koji mogu imati prekogranični efekat ili uticati na stabilnost finansijskog sistema, Komisija može zahtijevati dostavljanje dodatnih informacija ili koordinisano izvještavanje u saradnji sa drugim nadležnim tijelima.

Društvo za upravljanje vodi internu evidenciju o svim IKT incidentima, bez obzira na njihov značaj, koja sadrži datum, opis, procjenu uticaja i preduzete mjere, a evidencija se čuva najmanje pet godina i dostavlja Komisiji na zahtjev.

Komisija može propisati obrasce i tehničke formate za prijavu i dostavljanje obavještenja i izvještaja o IKT incidentima, radi standardizacije i efikasne komunikacije.

Napredna testiranja digitalne operativne otpornosti i izvještavanje Komisiji

Član 8

Društvo za upravljanje čije poslovanje ima veći obim, složenost ili značajnu zavisnost od informacionih sistema dužno je da, pored osnovnih testiranja iz člana 5 ovih pravila, sprovodi i napredna testiranja digitalne operativne otpornosti.

Napredna testiranja obuhvataju najmanje:

1. simulirane sajber napade i testiranja zasnovana na prijetnjama ("threat-led penetration testing", TIBER-like pristupe),
2. napredne provjere kontinuiteta poslovanja i oporavka, uključujući testove fizičkog oporavka sistema i infrastrukture,
3. integrisana testiranja više sistema i funkcija radi procjene ukupne otpornosti.

Napredna testiranja se sprovode na osnovu godišnjeg plana testiranja koji sadrži:

1. ciljeve, opseg i metodologiju testiranja,
2. odgovorna lica, izvore i rokove,
3. kriterijume za procjenu rezultata i plan korektivnih mjera.

O rezultatima naprednih testiranja društvo za upravljanje sačinjava izvještaj koji sadrži:

1. opis sprovedenih aktivnosti,
2. identifikovane ranjivosti i slabosti,
3. preduzete i planirane korektivne mjere,
4. procjenu uticaja na digitalnu operativnu otpornost.

Izvještaj iz stava 4 dostavlja se Komisiji najkasnije 30 dana od završetka testiranja.

Komisija može:

1. zahtijevati dodatna objašnjenja ili dokumentaciju,
2. naložiti sprovođenje dodatnih testova,
3. zahtijevati preispitivanje metodologije i obima testiranja,
4. odrediti obavezu učešća subjekta u koordinisanim testovima otpornosti.

Društvo za upravljanje dužno je da dokumentuju i čuvaju sve zapise o naprednim testiranjima najmanje pet godina.

Saradnja sa Komisijom i izvještavanje o sprovođenju mjera digitalne otpornosti

Član 9

Društvo za upravljanje dužno je da obezbijedi stalnu saradnju i razmjenu informacija sa Komisijom u vezi sa sprovođenjem mjera digitalne operativne otpornosti.

Društvo za upravljanje dostavlja Komisiji godišnji izvještaj o sprovođenju mjera digitalne otpornosti, koji obuhvata:

1. opis uspostavljenih politika, procedura i tehničkih kontrola u oblasti IKT bezbjednosti;
2. sažetak sprovedenih testiranja digitalne otpornosti i preduzetih korektivnih mjera;
3. pregled evidentiranih IKT incidenata, njihov uzrok i način otklanjanja;
4. stanje i ažuriranje planova kontinuiteta poslovanja i oporavka;
5. promjene u angažovanju IKT trećih lica i procjenu povezanih rizika;
6. ocjenu stepena usklađenosti sa ovim pravilima i internim politikama.

Izvještaj iz stava 2 dostavlja se Komisiji najkasnije do 31. marta tekuće godine za prethodnu kalendarsku godinu.

Komisija može zahtijevati dostavljanje vanrednog izvještaja ili dodatnih informacija o pojedinim incidentima, testiranjima ili ugovorima sa IKT trećim licima, ukoliko ocijeni da postoji povećani rizik po digitalnu otpornost društva za upravljanje.

Društvo za upravljanje dužno je da Komisiji, na njen zahtjev, obezbijedi pristup svim relevantnim dokumentima, evidencijama i zapisima o IKT sistemima, testovima, planovima kontinuiteta, ugovorima sa IKT trećim licima i drugim dokumentima od značaja za procjenu digitalne otpornosti.

Komisija može, u okviru svojih nadzornih ovlašćenja, sprovesti provjere na licu mjesta, zahtijevati sprovođenje dodatnih mjera i izdavati preporuke radi unapređenja sistema digitalne otpornosti.

Društvo za upravljanje dužno je da u roku koji odredi Komisija obavijesti o sprovedenim mjerama i preporukama, te da o tome sačine izvještaj o realizaciji preporuka.

Proporcionalnost i fazna primjena

Član 10

Mjere i zahtjevi propisani ovim pravilima primjenjuju se proporcionalno prirodi, obimu, složenosti i nivou izloženosti IKT rizicima društva za upravljanje.

Društvo za upravljanje koje ima manji obim poslovanja, jednostavniju strukturu sistema i manju izloženost IKT rizicima može, uz prethodno obrazloženje i dokumentovanu procjenu rizika, da primjenjuje pojednostavljene mjere u pogledu:

1. obima testiranja digitalne otpornosti,
2. učestalosti vježbi kontinuiteta poslovanja i oporavka,
3. načina izvještavanja o IKT incidentima,
4. sadržaja i detaljnosti godišnjih izvještaja Komisiji.

Komisija može, na osnovu dostavljene procjene rizika i kriterijuma koje propiše, odobriti pojednostavljenu primjenu određenih obaveza, ako ocijeni da to ne ugrožava stabilnost i sigurnost poslovanja.

Društvo za upravljanje dužno je da u roku od šest mjeseci od dana početka primjene ovih pravila usklade svoje politike, procedure i planove sa njegovim odredbama.

Za subjekte koji prvi put započinju poslovanje nakon početka primjene ovih pravila, obaveze iz čl. 3-9 primjenjuju se od dana dobijanja dozvole za rad.

Završne odredbe

Član 11

Ovaj pravila stupaju na snagu osmog dana od dana objavljivanja u "Službenom listu Crne Gore".

Primjena ovih pravila započinje od dana početka primjene odredaba Zakona o otvorenim investicionim fondovima sa javnom ponudom kojima se uređuje digitalna operativna otpornost društava za upravljanje.

Broj: 01/7-567/5-26

Podgorica, 2. 7. 2026. godine

Predsjednik Komisije,

Željko Drinčić, s.r.