BANKA QENDRORE E REPUBLIKËS SË KOSOVËS
CENTRALNA BANKA REPUBLIKE KOSOVO
CENTRAL BANK OF THE REPUBLIC OF KOSOVO

Na osnovu člana 35. stav 1. tačka 1.1 Zakona br. 03/L-209 o Centralnoj banci Republike Kosovo (Službeni list Republike Kosovo, br. 77/16. avgust 2010.), izmenjen i dopunjen Zakonom br. 05/L -150 o Centralnoj banci Republike Kosovo (Službeni list Republike Kosovo, br. 10/03 april 2017.), kao i člana 7. stav 7.4, tačka (c), člana 15. stav 15.7, tačka (e), i člana 22. stav 22.7, tačka (e), Zakona br. 04/L-101 o penzijskim fondovima na Kosovu (Službeni list Republike Kosovo, br. 10/8. maj 2012.), izmenjen i dopunjen Zakonom br. 05/L -116, o izmeni i dopuni Zakona br. 04/L-101 o penzijskim fondovima na Kosovu, izmenjen i dopunjen Zakonom br. 04/L-115 i Zakonom br. 04/L-168 (Službeni list Republike Kosovo br. 3/17. januar 2017.), Odbor Centralne banke je na sednici održanoj 28. februara 2024. godine usvojio sledeće:

UREDBA O SISTEMIMA I BEZBEDNOSTI INFORMACIJA PENZIJSKIH FONDOVA

Član 1.
Cilj i delokrug

1. Cilj ove Uredbe je da utvrdi minimalne kriterijume i uslove koje penzijski fondovi moraju da ispune za organizovanje i funkcionisanje svojih sistema informacione tehnologije (u daljem tekstu IT), koji omogućavaju smanjenje operativnog rizika koji se može prouzrokovati zloupotrebom IT sistema, kao i da sačuva pouzdanost ovih sistema u podršci aktivnostima penzijskih fondova. Minimalni kriterijumi i uslovi utvrđeni ovom Uredbom odnose se na upravljanje, bezbednost i rad informacionih sistema penzijskih fondova, kao i obezbeđivanje kontinuiteta rada u slučaju bilo kakvog nepredviđenog događaja.
2. Ova Uredba se primenjuje na penzijske fondove koji funkcionišu u Republici Kosovo, a koji se u daljem tekstu navode kao fond/ovi ili penzijski fond/ovi.

Član 2.
Definicije

1. Svi izrazi koji se koriste u ovoj Uredbi imaju isto značenje definisano članom 1. Zakona br. 04/L-101 o penzijskim fondovima na Kosovu i članom 1. Zakona br. 04/L-168 o izmeni i dopuni Zakona br. 04/L-101 o penzijskim fondovima na Kosovu i/ili sa definicijama za potrebe ove Uredbe kao u nastavku:
   1.1. **Informacioni sistem** – označava celokupnu tehnološku grupu koju čine infrastruktura (softverske i hardverske komponente), fondovi (institucija), ljudi i procedure za prikupljanje, obradu, prikaz i korišćenje podataka i informacija, prenos i skladištenje;
   1.2. **Korisnici informacionog sistema** – označava sva lica koja su ovlašćena za korišćenje informacionih sistema (zaposleni u instituciji, zaposleni u drugim preduzećima koji imaju pristup informacijama sistema penzijskih fondova);

1.3. **Penzijski fond** – označava Fond penzijske štednje, kao i druge penzione fondove licencirane od strane CBK-a.

1.4. **Softverske komponente** – označava sve vrste operativnog sistema, aplikativnog softvera, alata za razvoj softvera i drugih softverskih sistema;

1.5. **Hardverske komponente** – označava računarsku opremu, mrežnu opremu, medije za skladištenje podataka i drugu tehničku opremu, koja služi kao podrška radu informacionih sistema;

1.6. **Imovina** – označava materijalnu i nematerijalnu imovinu koja imaju vrednost za Penzijski fond.

1.7. **Čisti sto** – označava uklanjanje svih dokumenata i druge poverljive imovine sa radnog stola tokom perioda bez nadzora i na kraju radnog vremena.

1.8. **Spoljni pružalac usluga** – označava fizičko ili pravno lice koje na osnovu pisanog sporazuma pruža usluge fondu za funkcije koje mu je fond delegirao;

1.9. **Incident** – označava neplanirani događaj koji nije normalan deo operacija i koji prekida proces ili uslugu ili smanjuje kvalitet usluge;

1.10. **Zona servera** – označava zonu gde se uglavnom čuvaju i nalaze serveri i druga pomoćna oprema, potrebna za komunikacione usluge, signalizaciju i druge elektronske uređaje u kojima se čuvaju beleške banke.

1.11. **Međunarodno prihvaćeni standardi** – označava serija ISO/IEC 27000; NIST 800; COBIT; ITIL i slično.

1.12. **Cloud usluge** – označava infrastrukturne, prostorne i aplikativne resurse koji postoje na Internetu (eng. Infrastructure as a Service (IaaS), Platform as a Service (PaaS) i Software as a Service (SaaS)). Pružaoci ovih usluga/resursa sklapaju ugovor sa primaocima usluga kako bi im omogućili korišćenje računarskih resursa bez kupovine ili održavanja fizičke ili softverske opreme.

Član 3.
Upravljanje informacionim sistemima

1. Penzijski fond mora da uspostavi odgovarajući informacioni sistem koji mora da sadrži sledeće uslove:

1.1. Imati funkcionalnost, kapacitet i učinak koji pružaju podršku koja je potrebna procesima aktivnostima fonda;

1.2. Pruža blagovremene, tačne i potpune informacije za donošenje odluka institucije i upravljanje rizicima, radi omogućavanja sigurnosti i stabilnog funkcionisanja penzionog fonda;

1.3. Pruža odgovarajuću kontrolu verifikacije/validacije podataka, tokom procesa obrade i tokom ekstrakcije podataka, kako bi sprečio netačnosti i nedoslednosti u podacima i informacijama;

2. Penzijski fond vrši kontinuirano praćenje, regulisanje i unapređenje procesa upravljanja informacionim tehnologijama kako bi smanjio izloženost riziku uz održavanje njegove bezbednosti i funkcionalnosti.

Član 4.
Organizaciona struktura za upravljanje IT-om

1. Penzijski fond u svojoj organizacionoj strukturi mora uspostaviti IT jedinice sa dovoljnim brojem i odgovarajućim osobljem kako bi se osiguralo da se IT oblašću efikasno upravlja na osnovu međunarodno prihvaćenih standarda. Podela dužnosti treba da se izvrši u skladu sa međunarodno prihvaćenim standardima sa jasno definisanim odgovornostima i nadležnostima za proces upravljanja IT-om i bezbednošću informacija. Ova jedinica mora da dostavi redovne informativne izveštaje najmanje na tromesečnoj osnovi višem rukovodstvu penzijskog fonda.
2. Penzijski fond mora da odredi odgovorno lice za informacionu bezbednost koje mora da upravlja bezbednošću informacionog sistema i usklađuje politike i procese za informacionu bezbednost vezano za funkcije i tehnološke platforme. Odgovorno lice odgovara upravnom direktoru i mora biti nezavisno od drugih organizacionih jedinica. Odgovorno lice mora da podnosi izveštaje preko upravnog direktora najmanje jednom godišnje, a po potrebi i Upravnom odboru koji mora biti obavešten o operacijama i funkcijama u vezi sa bezbednošću informacija.
3. U slučaju delegiranja IT funkcija na spoljnog pružaoca usluga (eng. outsource), Penzijski fond mora imenovati najmanje jednog internog službenika specijalizovanog za oblast informacionih tehnologija, kao odgovornog za koordinaciju i nesmetano funkcionisanje IT funkcija.

Član 5.
Strategija, politike i procedure za upravljanje IT-om i bezbednost informacija

1. Penzijski fond utvrđuje strategiju i zahteve bezbednosti za rad IT sistema, politike za tehnologiju i bezbednost informacija, kao i procedure za procese iz oblasti.
2. Penzijski fond, u skladu sa strategijom institucije, donosi strategije razvoja IT sistema.
3. Upravni odbor je odgovoran za odobravanje politike tehnologije i bezbednosti informacija i najmanje jednom godišnje mora da proceni adekvatnost politika i izvrši njihovu reviziju.
4. Strategiju i politike za IT odobrava Odbor direktora, dok IT procedure odobrava više rukovodstvo.
5. U slučajevima kada penzijski fond sve ili deo svojih IT aktivnosti (ili sistema) obezbeđuje od spoljnih pružaoca usluga, tada penzijski fond usvaja internu proceduru za delegiranje funkcija kako bi obezbedio usklađenost sa zahtevima ove Uredbe za bezbednost i za pravilno funkcionisanje ovih sistema.
6. Interna procedura za delegiranje funkcija iz stava 5. ovog člana mora da sadrži najmanje sledeće elemente:

   6.1. Identifikovanje funkcija koje su delegirane i procenu uticaja koje delegiranja tih funkcija ima;

6.2. Procedure za delegiranje funkcija, uključujući kriterijume za izbor primaoca delegiranih funkcija;

6.3. Rokove i metode izveštavanja primaoca delegiranih funkcija fondu;

6.4. Načine praćenja primaoca delegiranih funkcija od strane penzionog fonda;

7. Politike i procedure za upravljanje IT-om treba da definišu najmanje sledeće elemente:

7.1. Administracija i rad IT sistema;

7.2. Organizaciona struktura za upravljanje IT-om;

7.3. Hardverska infrastruktura iz oblasti IT-a (konfiguracioni dijagrami);

7.4. Klasifikacija dokumentacije i zaštita sistema i podataka;

7.5. Rezervna kopija sistemskih podataka;

7.6. Upravljanje sistemskim promenama (eng. change management);

7.7. Upravljanje incidentima;

7.8. Upravljanje rizikom IT sistema;

7.9. Određivanje sigurnosnih mehanizama IT sistema;

7.10. Upravljanje trećim licima.

8. Penzijski fond mora da obezbedi primenu svih odobrenih internih politika i procedura u vezi sa IT, kao i da obezbedi da svi korisnici IT budu obavešteni o sadržaju ovih politika i procedura u skladu sa njihovim ovlašćenjima i odgovornostima.

Član 6.
Razvoj i nabavka IT sistema

1. Da bi umanjio rizik, Penzijski fond mora da prati trend razvoja sistema, vodeći računa da koristi samo verzije koje su ažurirane i podržane od njihovih pružalaca.
2. Penzijski fond mora da obezbedi izradu i odobrenje internih procedura o načinu na koji obavlja razvoj, promene, testiranje, validaciju i osiguranje kvaliteta da bi ublažio potencijalne ranjivosti ili operativne poremećaje u svojim IT sistemima. IT sistemi se *užívo* puštaju u rad tek nakon što specijalizovani službenik koji vrši proveru primenljivosti procedura i ispravnog funkcionisanja sistema da svoje pisano odobrenje.
3. Pre postavljanja sistema, treba izvršiti procenu rizika i analizu usklađenosti kako bi se osiguralo da sistem ispunjava zahteve bezbednosti, rada i funkcionalnosti.
4. U slučajevima nabavke sistema, Fond mora da sledi standardizovani proces javnih nabavki. Ovaj proces treba da obuhvati temeljnu procenu ugleda dobavljača, finansijske stabilnosti i rezultata u obezbeđivanju sigurnih i pouzdanih softverskih rešenja. Sporazumi treba da jasno opisuju očekivanja Fonda u vezi sa merama bezbednosti, sporazumima o nivou usluga i zahtevima za zaštitu podataka.
5. Ako Fond izabere razvoj internog softvera, mora da uspostavi proces životnog ciklusa razvoja softvera (SDLC). Ovaj proces treba da uključi identifikaciju i primenu bezbednih praksi kodiranja, redovne preglede koda, procene ranjivosti i testiranje u svakoj fazi razvoja. Fond

takođe treba da uspostavi mehanizme za stalno održavanje, ažuriranje i praćenje rada i bezbednosti softvera.

6. Spoljni pružalac usluga tokom implementacije i rada na sistemima ni na koji način ne bi trebalo da ima pristup verzijama sistema koji su u produkciji (uživo). Izvođači i druge spoljne strane treba da testiraju sve promene u okruženju za testiranje.

Član 7.
Delegiranje IT funkcija spoljnim pružaocima usluga

1. Penzijski fond je odgovoran da obezbedi da se IT delatnost obavlja u skladu sa svim zahtevima definisanim ovom Uredbom, čak i u slučajevima kada celu ili deo IT delatnosti obavljaju spoljni pružaoci IT usluga.
2. Pre izbora spoljnog pružaoca IT usluga, Fond treba da preduzme sledeće aktivnosti:
   2.1. Utvrđivanje minimalnih standarda koje spoljni pružalac IT usluga mora da ispuni i koji moraju biti usklađeni sa planom kontinuiteta poslovanja;
   2.2. Sprovođenje procene rizika poslovanja penzionog fonda koji može nastati korišćenjem spoljne usluge koja se pruža tokom obrade aktivnosti penzionog fonda;
   2.3. Utvrđivanje načina nadgledanja usluge i kvaliteta poslovanja kompanije, finansijske situacije i profila rizika kroz periodično testiranje usklađenosti sa politikom bezbednosti informacionog sistema;
   2.4. Da pravilno utvrdi delatnost spoljnog pružaoca IT usluga sa pravnog i finansijskog aspekta, kao i sa aspekta upravljanja bezbednošću informacionog sistema definisanog ovom Uredbom;
   2.5. Definisanje koordiniranog upravljanja bezbednosnim incidentima.
   2.6. Određivanje neophodnih mera za izbegavanje sukoba interesa;
3. Sporazum između penzionog fonda i spoljnog pružaoca IT usluga treba da bude definisan pisanim ugovorom koji, između ostalog, treba da sadrži:
   3.1. Podatke o povezanim licima (Penzijski fond i spoljni pružalac IT usluga);
   3.2. Opis delegiranih funkcija;
   3.3. Prava i obaveze povezanih lica;
   3.4. Rukovanje i održavanje poverljivosti podataka;
   3.5. Rokove za pružanje usluge i otkazni rok za raskid ugovora koji je dovoljan za pronalaženje alternativnih rešenja;
   3.6. Ugovor o nivou usluge (eng. Service level agreement);
   3.7. Odredbu koja određuje da će spoljni pružalac IT usluga biti predmet nadzora CBK-a u vezi sa delegiranim IT aktivnostima;
   3.8. Odredbu kojom se utvrđuje da pružaoci IT usluga obavljaju svoje aktivnosti u skladu sa zakonima na snazi, zahtevima, regulatorima, kao i politikama odobrenim od Penzijskog fonda i da sarađuju sa CBK-om u smislu delegiranih funkcija;

3.9. Pravo Penzijskog fonda da bude informisan od strane spoljnog pružaoca IT usluga o napretku funkcija, kao i pravo Fonda da daje opšta ili posebna uputstva u vezi sa obavljanjem delegiranih funkcija;

3.10. Pravo Penzijskog fonda da vrši inspekciju i kontrolu aktivnosti spoljnog pružaoca IT usluga u vezi sa delegiranim IT aktivnostima.

3.11. Obavezu spoljnog pružaoca IT usluga da odmah obavesti Penzijski fond o svakoj činjenici koja može imati značajan uticaj na njegovu sposobnost da efikasno i delotvorno obavlja svoju delatnost u skladu sa zakonskim zahtevima na snazi;

4. Spoljni pružalac usluga ne može podugovarati usluge osim ako nije navedeno u osnovnom ugovoru zaključenom između Penzijskog fonda i ovog pružaoca usluga.
5. Penzijski fond je dužan da upravlja rizicima koji proizilaze iz ugovornih odnosa sa spoljnim pružaocima usluga čije su aktivnosti vezane za informacioni sistem koji koristi Penzijski fond.
6. Penzijski fond je dužan da kontinuirano prati način i kvalitet aktivnosti ugovorenih od strane spoljnog pružaoca.

Član 8.
Bezbednost informacionih sistema

1. Bezbednost informacionih sistema zasniva se na utvrđivanju ispunjenosti sledećih kriterijuma:

   1.1. Poverljivost: informacije moraju biti dostupne samo ovlašćenim korisnicima;

   1.2. Integritet: održavanje tačnosti i potpunosti informacionog sistema;

   1.3. Dostupnost: pristup informacionom sistemu u svakom trenutku za ovlašćene korisnike.

2. Penzijski fond mora kontinuirano da upravlja procesom bezbednosti informacionog sistema. Penzijski fond mora da identifikuje i prati potrebe za bezbednošću informacionog sistema, u najmanju ruku na osnovu rezultata procene rizika tog sistema i obaveza koje proizilaze iz internih akata ili ugovornih odnosa.
3. Penzijski fond mora da utvrdi postupke, metode i kriterijume za klasifikaciju informacija prema stepenu osetljivosti i relevantnosti – u odnosu na moguće posledice povrede poverljivosti, njihovog integriteta i dostupnosti.
4. Penzijski fond mora da obezbedi da informaciona bezbednost i sve aktivnosti vezane za nju moraju biti u skladu sa svim važećim zakonima koji se odnose na informisanje i poslovanje institucije.

Član 9
Bezbednost u uslugama *cloud* prostora

1. Primalac *cloud* usluga mora pripremiti i definisati politiku i proceduru za upravljanje *cloud* uslugama.
2. Pružaoci *cloud* usluga moraju imati iskustvo i pozitivnu reputaciju u pružanju *cloud* usluga.
3. Pružaoci *cloud* usluga moraju da se pridržavaju međunarodno prihvaćenih standarda kako bi osigurali bezbednost, integritet i poverljivost podataka koji se obrađuju, čuvaju ili prenose preko

njihovih platformi, uvek poštujući prakse, procedure i politiku bezbednosti informacija korisnika usluga, kao i pridržavajući se svih važećih zakona i propisa. Pružaoci ovih usluga moraju uspostaviti sveobuhvatne mere bezbednosti koje uključuju klasifikaciju i zaštitu podataka, kontrolu pristupa, metode šifrovanja, plan i procedure za reagovanje na incidente, kao i plan oporavka od katastrofe i kontinuiteta rada.

4. Primaoci usluga u *cloud* prostorima moraju da procene bezbednosne mere koje sprovode pružaoci *cloud* usluga i redovno prate njihovu usklađenost kako bi ublažili potencijalne rizike koji ugrožavaju bezbednost podataka ili neovlašćeni pristup.
5. Kontrole bezbednosti primaoca usluge (operativne, proceduralne ili tehničke procedure za zaštitu integriteta, poverljivosti i tačnosti podataka i informacionih sistema primaoca usluge) mora da sprovodi pružalac *cloud* usluga na korektan i efikasan način.
6. Pružaoci *cloud* usluga moraju da obezbede *cloud* prostor koji je fizički odvojen od prostora drugih korisnika, te moraju da poseduju procedure i politike za prikupljanje i čuvanje revizorskih tragova kako bi osigurali da se svaka aktivnost efikasno nadgleda.
7. Daljinski pristup informacionim sistemima koji se nalaze u *cloud* prostorima mora biti omogućen metodama za autentifikaciju sa dva ili više faktora (eng. Multi-factor authentication). Komunikacija između uređaja koji daljinski pristupa uslugama/resursima hostovanim u *cloud*-u mora da ima uspostavljeno mere enkripcije *end-to-end* za svaku sesiju komunikacije.
8. Konfiguracije infrastrukture, lista usluga/resursa koji se nude u *cloud* prostorima, kao i lista aplikacija koje rade u *cloud* prostorima treba da budu transparentne i detaljno dokumentovane.
9. Pružalac *cloud* usluga mora da obezbedi proceduru i politiku za kreiranje, testiranje i zaštitu rezervnih kopija koje su u skladu sa politikama i procedurama primaoca usluge.
10. U slučaju da dođe do neovlašćenog pristupa ili bilo kakvog bezbednosnog incidenta, od pružalaca *cloud* usluga se zahteva da takve incidente odmah prijave regulatornim vlastima i primaocu usluge.
11. Pružaoci *cloud* usluga moraju da obezbede transparentnu dokumentaciju o svojim bezbednosnim praksama i da ovu dokumentaciju učine dostupnom za pregled tokom procesa ispitivanja ili revizije.
12. Potrebno je uraditi test *prodiranja* i procene ranjivosti i mogućih bezbednosnih rizika u vezi sa čuvanjem podataka i informacionih sistema u *cloud* prostorima najmanje jednom godišnje.
13. Pružalac usluga mora posedovati politiku ili proceduru za bezbedno brisanje podataka (eng. Secure data deletion) i uništavanje infrastrukture u slučaju raskida ugovora ili uklanjanja resursa usluge iz upotrebe.
14. CBK ima pravo da sprovodi redovne preglede i procene pružalaca *cloud* usluga u penzijskoj industriji kako bi proverila usklađenost sa standardima bezbednosti informacija i najboljim praksama.

Svi zahtevi ove Uredbe za informacione sisteme shodno se primenjuju i na pružaoce *cloud* usluga koji se odnose na usluge u *cloud* prostorima.

Član 10.
Upravljanje rizikom za informacione sisteme

1. Penzijski fond utvrđuje kriterijume za dozvoljeni rizik u vezi sa korišćenjem svojih informacionih sistema prema međunarodno prihvaćenim standardima.
2. Najmanje jednom godišnje ili u slučaju značajnih promena u zahtevima bezbednosti informacija, Penzijski fond sprovodi analizu rizika informacionih sistema kako bi obezbedio da se ovaj rizik održava u prihvatljivim granicama vezanim za delatnost Fonda. Rezultati analize rizika se dokumentuju.
3. Proces procene rizika uključuje, ali nije ograničen na, sledeće korake:
   3.1. Identifikacija sistemskih zahteva i ciljeva.
   3.2. Procena ranjivosti i potencijalnih bezbednosnih rizika povezanih sa sistemom.
   3.3. Procena potencijalnog uticaja na poslovanje fonda, privatnost podataka i poverljivost subjekta podataka.
   3.4. Procena kompatibilnosti sistema sa drugim sistemima i postojećom infrastrukturom.
   3.5. Procena proširivosti, pouzdanosti i održivosti sistema.
   3.6. Analiza potencijalnih pitanja usklađenosti sa zakonima i propisima.
   3.7. Procena finansijskih i resursnih implikacija interne implementacije, nabavke ili razvoja.
4. Na osnovu rezultata procene rizika, Fond mora da izradi plan ublažavanja rizika koji opisuje neophodne mere za minimiziranje identifikovanih rizika. Plan za smanjenje rizika treba da uključuje, ali ne ograničavajući se na:
   4.1. Sprovođenje odgovarajućih mera bezbednosti za zaštitu podataka.
   4.2. Izradu procedura za pravljenje rezervnih kopija i oporavak podataka.
   4.3. Integraciju sistema sa drugim sistemima i postojećom infrastrukturom.
   4.4. Pružanje neophodne obuke i podrške zaposlenima uključenim u sprovođenju, nabavku ili razvoj softvera.
   4.5. Usklađenost sa relevantnim zakonskim i regulatornim zahtevima.
   4.6. Izdvajanje adekvatnih finansijskih i ljudskih resursa kako bi se osiguralo uspešno interno sprovođenje, nabavka ili razvoj.
5. Fondovi treba da redovno pregledaju i ažuriraju procenu rizika i plan za smanjenje rizika tokom životnog ciklusa softvera kako bi se pozabavili svim novim rizicima ili promenama u zahtevima Fonda i operativnom okruženju.
6. Penzijski fond mora pismenim putem obavestiti CBK u slučaju identifikacije incidenata, u informacionim sistemima i promenama u ključnim funkcijama važnih procesa informacionih sistema koji mogu ometati ili ugroziti instituciju, najkasnije jedan radni dan nakon dešavanja incidenta.
7. Upravljanje rizicima informacionog sistema treba da obuhvati celokupni informacioni sistem integrisanog fonda u svim fazama njegovog razvoja.

8. Upravljanje rizikom informacionog sistema mora da sadrži godišnji plan podizanja svesti zaposlenih u Fondu za adekvatno korišćenje usluga koje se pružaju preko informacionog sistema fonda.

Član 11.
Fizička bezbednost informacionih sistema

1. Penzijski fond mora preduzeti neophodne mere bezbednosti da spreči svaki neovlašćeni fizički pristup, mešanje ili oštećenje informacija, opreme za obradu informacija i operacija Fonda na osnovu međunarodno prihvaćenih standarda.
2. Penzijski fond mora uspostaviti pristup i procedure rada za bezbednosne oblasti za sve zaposlene i spoljne strane. Bezbednosne oblasti moraju biti zaštićene kontrolom pristupa kako bi se osiguralo da samo ovlašćeni zaposleni imaju pristup.
3. Takođe treba odrediti mere bezbednosti za opremu koja se koristi i postavlja van objekata penzionog fonda u zavisnosti od lokacije i uzeti u obzir rizike prilikom određivanja neophodnih kontrola.
4. Oprema se mora održavati da bi se zaštitila od kvarova, da bi se obezbedila stalna dostupnost i integritet, i da bi izdržala prekide kao rezultat kvarova na pomoćnoj opremi, prirodnih katastrofa, zlonamernih ili slučajnih napada itd.
5. Svi uređaji koji sadrže informacije moraju biti verifikovani kako bi se osiguralo da su svi podaci i licencirani softver uklonjeni pre odlaganja, uništenja ili ponovne upotrebe kako bi se sprečilo vraćanje originalnih informacija.
6. Svi korisnici moraju biti upoznati sa bezbednosnim zahtevima i procedurama za zaštitu opreme bez nadzora.
7. Fond mora da definiše kriterijume, metode i procedure za čisti sto u cilju zaštite informacija.
8. Ugovorne obaveze za zaposlene i spoljne pružaoce IT usluga treba da odražavaju politiku informacione bezbednosti Penzijskog fonda. Svi zaposleni i spoljni pružaoci IT usluga moraju razumeti odgovornosti za uloge koje se razmatraju.
9. Tamo gde je pogodno za primenu, Fond utvrđuje da zaposleni i spoljni pružaoci usluga zadržavaju informacije dobijene tokom obavljanja svoje delatnosti u određenom periodu nakon raskida ugovora sa zaposlenim ili spoljnim pružaocima IT usluga.
10. Fond mora da odredi radnje i mere koje treba preduzeti u slučaju kršenja bezbednosnih zahteva od strane zaposlenih ili spoljnih pružaoca IT usluga.

Član 12.
Upravljanje računarskim mrežama

1. Računarska mreža Fonda se mora upravljati i kontrolisati u cilju zaštite informacija sistema i aplikacija. Fond mora da sprovodi kontrole radi obezbeđivanja zaštite poverljivosti i integriteta informacija na mreži i zaštite usluga od neovlašćenog pristupa na osnovu međunarodno prihvaćenih standarda.
2. Za upravljanje računarskim mrežama Fond mora da utvrdi:

2.1. Procedure korišćenja i upravljanja mrežnim servisima i uređajima u cilju ograničavanja pristupa mrežnim servisima i aplikacijama;

2.2. Uspostavljanje posebnih kontrola za zaštitu poverljivosti i integriteta podataka koji prolaze kroz javne ili bežične mreže (eng. wireless);

2.3. Tehnologiju primenjenu na bezbednost mrežnih usluga kao što su provera autentičnosti, šifrovanje i kontrole mrežne veze;

2.4. Grupe informacionih servisa, korisnika i informacionih sistema moraju biti izolovane od javnih mreža;

2.5. Posebne kontrole treba posvetiti pristupu spoljnih pružalaca usluga u slučajevima potrebe za interkonekcijom (veze sa trećim licima).

Član 13.
Upravljanje imovinom informacionih sistema

1. Fond mora da identifikuje svu imovinu u informacionim sistemima.
2. Fond mora da održava inventar celokupne imovine sa svim potrebnim informacijama, uključujući vrstu imovine, format, lokaciju, rezervne informacije (gde je primenjivo), informacije o licenci i poslovnu vrednost.
3. Fond mora da utvrdi i dokumentuje vlasništvo i klasifikaciju celokupne imovine koja se odnosi na obradu informacija.
4. Vlasnik imovine je odgovoran za:

   4.1. Obezbeđivanje da su informacije i imovina u vezi sa obradom informacija klasifikovane prema osetljivosti;

   4.2. Definisanje i redovan pregled ograničenja pristupa i klasifikacije.
5. Fond mora da utvrdi pravila o prihvatljivom korišćenju informacija i imovina koja se odnose na obradu informacija.

Član 14.
Upravljanje pristupom korisnika

1. Fond upravlja pristupom informacionim sistemima kroz relevantne interne procedure za upravljanje pravima pristupa korisnika. Interne procedure moraju da sadrže kriterijume za pristup, ovlašćenje, identifikaciju i autentifikaciju korisnika prema međunarodno prihvaćenim standardima.
2. Svaki korisnik mora biti jedinstven i sistem mora definisati kriterijume za postavljanje lozinke prema međunarodno prihvaćenim standardima. Pre odobravanja pristupa informacionim sistemima, kako interni zaposleni u fondu tako i spoljni pružaoci usluga moraju da potpišu ugovore o poverljivosti i neotkrivanju podataka.
3. Fond mora da obezbedi da dozvolu pristupa korisnika informacionim sistemima vrše odgovorna lica tih sistema i da se zasniva na principu najnižeg mogućeg pristupa sistemu, omogućavajući obavljanje radnih zadataka. Fond mora najmanje na 6 meseci da preispituje prava pristupa

korisnika sistemima od velikog značaja na osnovu procene rizika i najmanje jednom godišnje svim ostalim sistemima.

4. U upravljanju pravima pristupa korisnika, Fond mora posebno ovlastiti privilegovani pristup i/ili daljinski pristup informacionom sistemu. Sav pristup i aktivnost privilegovanih korisnika i daljinski pristup moraju biti nadgledani.
5. Daljinski pristup informacionim sistemima mora biti omogućen metodama za autentifikaciju sa dva ili više faktora (eng. Multi-factor authentication). Komunikacija između uređaja koji daljinski pristupa informacionom sistemu mora da ima mere enkripcije *end-to-end* za svaku komunikacijsku sesiju.
6. Penzijski fond mora da prati i skladišti događaje (eng. events) bezbednosti informacija u svojoj infrastrukturi na osnovu međunarodno prihvaćenih standarda.

Član 15.
Čuvanje informacija

1. Čuvanje informacija (backup) mora se obaviti prema internim procedurama Penzionog fonda.
2. Interni akti iz stava 1. ovog člana moraju da sadrže najmanje sledeće elemente:
   2.1. Postavljanje potrebnog nivoa rezervne kopije informacija;
   2.2. Čuvanje tačnih i potpunih podataka o rezervnoj kopiji informacija, kao i dokumentovanih procedura povratka rezervnih kopija;
   2.3. Vrstu (eng. Full, incremental, differential) i učestalost pravljenja rezervnih kopija prema složenosti posla.
3. Raspored pravljenja rezervnih kopija treba da bude zakazano kako bi se osiguralo da se sve informacije i softver mogu oporaviti u slučaju katastrofe ili kvara opreme.
4. Rezervne kopije treba da se čuvaju na drugoj lokaciji, dovoljno daleko da ne budu ugrožene od istih pretnji kao centralna lokacija.
5. Rezervne kopije moraju biti obezbeđene sa odgovarajućim nivoom fizičke i ekološke zaštite u skladu sa standardom koji se primenjuje na centralnoj lokaciji.
6. Rezervne kopije treba redovno testirati, osiguravajući da su pouzdane i upotrebljive kada je to potrebno.
7. Rezervne kopije moraju biti zaštićene od neovlašćenog pristupa putem šifrovanja.
8. Trajanje čuvanja informacija mora biti u skladu sa zakonima na snazi.

Član 16.
Interna revizija informacionog sistema

1. Na reviziju informacionog sistema primenjuju se zahtevi definisani propisom za interne kontrole i internu reviziju.
2. Aktivnost IT oblasti treba da bude predmet najmanje godišnje periodične revizije koja se fokusira na metodologiju zasnovanu na riziku.

3. IT revizije moraju da obavljaju nadležna lica u okviru funkcije interne revizije ili eksterna lica angažovana u ovu svrhu.
4. Svi zahtevi ove uredbe i odredbe iz stava 1. ovog člana ostaju na snazi u slučajevima kada se ugovaraju poslovi interne revizije.

Član 17.
Prostorija za servere

1. Prostorija za servere mora biti odvojena od ostalih kancelarija Penzijskog fonda i mora se nalaziti unutar objekata Fonda.
2. Da bi se omogućilo očuvanje evidencije i kontinuitet poslovanja (kao back-up) u slučaju prirodnih nepogoda ili katastrofa, Fond mora da odredi drugu rezervnu lokaciju, na kojoj se nalaze potrebni serveri. Ova rezervna lokacija mora se nalaziti na udaljenosti od glavnog centra Fonda, prema međunarodno prihvaćenim standardima u ovoj oblasti.
3. Penzijski fond u svojoj centralnoj prostoriji servera i rezervnoj lokaciji za skladištenje zapisa mora da ispunjava sledeće bezbednosne zahteve prostorije za servere:
   3.1. da ima neophodnu opremu za održavanje temperature na odgovarajućem nivou;
   3.2. da ima neophodnu opremu za održavanje vlažnosti na odgovarajućem nivou;
   3.3. da ima elektronsku zaštitu sa:
      3.3.1. seizmičkim senzorima;
      3.3.2. senzorima pokreta;
      3.3.3. senzorima za dim.
   3.4. da ima sistem za nadzor kamera za:
      3.4.1. ulaz u ovu prostoriju; i
      3.4.2. unutrašnjost ove prostorije.
   3.5. da ima protivpožarnu zaštitu.
   3.6. da bude opremljena drugim i kontinuiranim izvorom električne energije.
4. Prostorija za servere mora biti ograničena za pristup samo ovlašćenom osoblju sa metodama za autentifikaciju sa dva ili više faktora i nadgledana kroz ulazak/izlazak osoblja i spoljnih lica u ove prostorije.
5. Penzijski fond mora odrediti uslove pristupa osoblja i trećih lica ovlašćenih za pristup prostoriji za servere u slučaju vanrednih situacija.
6. Na zahtev Fonda, Centralna banka Republike Kosovo može da napravi izuzetke od nekih zahteva navedenih u stavu 3. ovog člana, ali istovremeno CBK može kontinuirano zahtevati ispunjenje minimalnih bezbednosnih uslova za određene kancelarije.

Član 18.

Kontinuitet rada nakon prekida kao posledica vanrednih događaja

1. Penzijski fond mora uspostaviti proces upravljanja kontinuitetom poslovanja kako bi osigurao nesmetan i kontinuiran rad svih kritičnih sistema i procesa, kao i ograničio gubitke u uslovima neregularnog poslovanja na osnovu međunarodno prihvaćenih standarda.
2. Penzijski fond mora da upravlja kontinuitetom rada na osnovu analize uticaja aktivnosti i procene rizika, koja mora da obuhvati:
   2.1. Utvrđivanje kritičnih procesa neophodnog rada za nesmetan i kontinuiran rad Penzionog fonda;
   2.2. Utvrđivanje resursa i sistema neophodnih za obavljanje pojedinih radnih procesa, kao i veza i zavisnosti između njih;
   2.3. Procena rizika za svaki od pojedinačnih procesa rada, kao i verovatnoća dešavanja neželjenih slučajeva i njihov uticaj na kontinuitet rada, finansijske gubitke i ugled Penzijskog fonda;
   2.4. Utvrđivanje nivoa prihvatljivih rizika i tehnika za ublažavanje identifikovanih rizika;
   2.5. Utvrđivanje trajanja prihvatljivog prekida rada za svaki od procesa.
3. Penzijski fond mora da odobri plan analize uticaja na poslovanje (BIA) koji analizira prekid aktivnosti, koji sadrži najmanje:
   3.1. Procese koji imaju najveći prioritet, kao i resurse potrebne za ove procese;
   3.2. Završne aktivnosti koje treba postići (eng. Service Delivery Objective);
   3.3. Konačno vreme oporavka (eng. Recovery Time Objective);
   3.4. Cilj tačke oporavka (ang. Recovery Point Objective).
4. Upravni odbor Penzijskog fonda mora na godišnjem nivou da odobrava Plan kontinuiteta poslovanja, kao i Plan oporavka od katastrofe, kojim se uređuje stvaranje uslova za oporavak i dostupnost resursa informacionog sistema neophodnih za odvijanje kritičnih poslovnih procesa.
5. Plan kontinuiteta poslovanja i oporavka od katastrofe treba da sadrži najmanje sledeće zahteve:
   5.1. procedure koje treba preduzeti u slučaju prekida rada sistema;
   5.2. ažuriranu listu svih potrebnih ljudskih i tehničkih resursa za ponovno uspostavljanje kontinuiteta poslovanja;
   5.3. podatke o odgovornim licima i njihovim zamenicima koji su odgovorni za oporavak poslovanja u slučaju nepredviđenih događaja, uključujući njihove definisane dužnosti i odgovornosti, kao i plan unutrašnjih i spoljnih komunikacija;
   5.4. alternativnu lokaciju u slučaju prekida poslovanja i oporavka u funkciji poslovnih procesa na primarnoj lokaciji. Ova lokacija treba da ima odgovarajuću udaljenost od primarnog centra, kako bi se izbegao uticaj istih opasnosti na obe lokacije.
6. Za sprovođenje planova iz stava 5. ovog člana, Penzijski fond obezbeđuje da svi zaposleni budu upoznati sa svojim ulogama i odgovornostima u hitnim slučajevima.

7. Penzijski fond usklađuje planove sa poslovnim promenama, uključujući promene proizvoda, aktivnosti, procesa i sistema, sa promenama u okruženju, kao i sa poslovnom politikom i poslovnom strategijom.
8. Penzijski fond proverava planove, najmanje jednom godišnje i nakon pojave značajnih promena, kao i dokumentuje rezultate tih testiranja.
9. U upravljanju kontinuitetom poslovanja, Penzijski fond uzima u obzir poslove poverene trećim licima i zavisnost od usluga ovih lica.
10. U slučaju okolnosti koje zahtevaju sprovođenje plana kontinuiteta poslovanja i plana za aktivnosti oporavka u slučaju katastrofe, Penzijski fond će obavestiti Centralnu banku Republike Kosovo, najkasnije narednog dana nakon nastanka takve okolnosti. Centralna banka Republike Kosovo može zahtevati dodatnu dokumentaciju u vezi sa relevantnim činjenicama u vezi sa ovim okolnostima i odrediti rok za podnošenje ovog dokumenta.

Član 19.
Dokumentovanje IT delatnosti

Penzijski fond vodi kompletnu i ažurnu dokumentaciju organizacije, opreme, sistema, pristupa i drugih važnih faktora vezanih za IT delatnost. Takva dokumentacija dokazuje da je usaglašenost sa zahtevima ove uredbe kontinuirana.

Član 20.
Popravne mere

Svako kršenje odredbi ove Uredbe podleže popravnim i kaznenim merama kako je definisano u Zakonu o Centralnoj banci Republike Kosovo i Zakonu o penzijskim fondovima na Kosovu.

Član 21.
Stupanje u snagu

1. Ova Uredba stupa na snagu danom usvajanja.
2. Penzijski fondovi moraju obezbediti usklađenost sa svim važećim odredbama do 30. juna 2024. godine.

Bashkim Nurboja
Predsednik Odbora Centralne Banke Republike Kosovo